SEVEN DEFENSE PRIORITIES FOR THE NEW ADMINISTRATION

Report of the Defense Science Board

This report summarizes the main findings and recommendations of reports published by the Defense Science Board for the Secretary of Defense during the last dozen years. The purpose of this effort is to aid the incoming Administration to make a fast start in addressing pressing national security issues and opportunities.

SEVEN DEFENSE PRIORITIES FOR THE NEW ADMINISTRATION

The United States has the most powerful, precise, and professional armed forces in the world. Nevertheless our military is challenged: Russia, China, Iran, and the Democratic People's Republic of Korea roil the World Order. Terrorists operate by global franchise, and groups like the Islamic State of Iraq and the Levant (ISIL) attempt to establish caliphates. Deterring nuclear war, arguably the highest priority for the Department of Defense (DoD), is complicated by new potential routes to nuclear escalation. States deterred by U.S. military might are pursuing asymmetric strategies of "gray zone" conflict: war short of all-out war. Long-term commitments to missions of stabilization, reconstruction, peacekeeping and nation building consume human and financial military resources for decades. New weapons like cyber and autonomous systems are aimed at the heart of the U.S. military strategy predicated on technological superiority; but also offer the U.S. an opportunity to grasp.

The Defense Science Board (DSB), an advisory body for the Secretary of Defense and other senior DoD officials, is chartered to address such challenges, including the most irksome problems and potent opportunities, unstructured and consequential, that involve science and technology; and almost always touch on policy, strategy, acquisition, manufacturing, operational concepts, and rules of engagement.

This report summarizes the main findings and recommendations of reports published by the Defense Science Board for the Secretary of Defense during the last dozen years. The purpose of this effort is to aid the incoming Administration to make a fast start in addressing pressing national security issues and opportunities. While the topics that have been addressed span a wide range, seven major themes dominated the Board's considerations.

1. **Protecting the homeland** against non-state actors; against enemy states in time of war; and against weapons of mass destruction and cyber;

2. **Deterring the use of nuclear weapons** to prevent nuclear war;

3. **Preparing for gray zone conflicts** as war short of all-out war becomes the norm;

4. **Maintaining information superiority** and what the information infrastructure enables for adversaries and for the U.S.;

5. **Anticipating intelligent systems and autonomy** including numbers and disaggregation, range, and danger on and above the sea surface that drives warfare undersea;

6. **Supporting stabilization, reconstruction, peacekeeping, and nation building** to win the peace; and

7. **Preparing for surprise** to the U.S. and by the U.S.

The themes are elaborated as defense priorities in the seven chapters that follow. Each chapter references the in-depth reports underlying those seven themes. Note that the seven themes are not, and could not be, fully independent of each other, and the first is no more or less imperative than the last.

The Board prepared its last summation at the beginning of the Obama Administration: *Defense Imperatives for a new Administration (2008)* and *Creating a DoD Strategic Acquisition Platform (2009)*. Some things have changed, some things have not changed.

LEADERSHIP OF THE DEFENSE SCIENCE BOARD

2001–2009

Honorable William Schneider, Jr., Chairman

Mr. Vincent Vitto, Vice Chairman

2009–2014

Honorable Paul G. Kaminski, Chairman

General Lester Lyles, U.S. Air Force (retired), Vice Chairman

2014–present

Dr. Craig Fields, Chairman

Dr. Eric Evans, Vice Chairman

CONTRIBUTORS

Dr. Michael Anastasio

Mr. Christopher Day

Dr. Eric Evans

Dr. Craig Fields

Mr. James Gosler

Dr. Miriam John

Honorable Anita Jones

Dr. Ronald Kerber

Honorable William LaPlante

Honorable Judith Miller

Honorable William Schneider

Mr. James Shields

Dr. Ralph Semmel

Mr. Robert Stein

Dr. James Tegnelia

TABLE OF CONTENTS

INTRODUCTION

INTRODUCTION

The Defense Science Board (DSB) provides the Secretary of Defense, the Deputy Secretary of Defense, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), the Chairman of the Joint Chiefs of Staff, and other senior officials including the Secretaries of the Military Departments and the Commanders of the Combatant Commands with independent advice and recommendations on critical national security issues involving science and technology.

The DSB addresses the Secretary's most irksome problems and potent opportunities, unstructured and consequential, that involve science and technology; and almost always also involve to a degree policy, strategy, acquisition, manufacturing, operational concepts and rules of engagement.

All members of the DSB have strong science and technology backgrounds, and are either former senior military officers, senior executives from defense and commercial industry, university professors, former senior officials from the Department of Defense and the intelligence community, national laboratories, and leaders from Federally Funded Research and Development Centers. DSB began in 1956: 2016 is its 60th anniversary.

During the last dozen years the DSB published a number of reports for the Secretary, and

this report summarizes the main findings and recommendations of those efforts. The purpose of the report is to assist the incoming Administration to make a fast start in addressing pressing national security issues and opportunities.

While the topics that have been addressed span a wide range, seven major themes dominated the DSB's considerations. They are listed below, and elaborated in the seven chapters that follow, which also reference the in-depth reports underlying those seven themes.

The DSB's prepared its last summation at the beginning of the Obama Administration: *Defense Imperatives for a New Administration (2008)* and *Creating a DoD Strategic Acquisition Platform (2009)*. Some things have changed, some things have not changed.

These are the seven major themes of the DSB's work during the last dozen years. Note that they are not, and could not be, fully independent of each other.

1. Protecting the Homeland

Against non-state actors

Against enemy states in time of war

Against weapons of mass destruction and cyber

Since 9/11, the U.S. can no longer be considered a sanctuary. The DoD's highest priority is protection of the homeland. The DSB published a number of reports to clarify DoD's roles and to assess its posture for defending the homeland and protecting it from new forms of threats that evolved since the Cold War. This chapter highlights DoD's dependence on critical domestic infrastructure, the supporting capabilities the Department will need to provide to civil authorities in times of disaster, and opportunities for improvement in the interagency.

The DSB has published reports characterizing how the threat to the homeland evolved since the end of the Cold War. Actors—and their tools—have proliferated beyond nation states. More nations will have missiles with range or delivery mechanisms that threaten the U.S. homeland. The cyber threat grows exponentially and can be promulgated with serious harm by individuals. Advances in technology can place even weapons of mass destruction—nuclear, chemical, and biological—in the hands of any state or non-state actor who desires them. DSB continually investigates what to do about these threats, defensively and offensively, at home and abroad.

The DSB is particularly concerned with the apparent belief that armed combat will always occur in somebody else's backyard and will never spread to the homeland. That is unlikely to be true.

2. Deterring the Use of Nuclear Weapons

Preventing nuclear war

Despite the "peace dividend" at the end of the Cold War, the DSB remains uncertain that downgrading the nation's nuclear deterrent would lead other nations to do the same, even as advances in the U.S.' non-nuclear warfighting capabilities proved their effectiveness. In fact, U.S. conventional dominance demonstrated in Bosnia, Iraq, and Afghanistan appears to have catalyzed a greater interest in nuclear weapons by others who do not have the resources to overmatch the U.S. otherwise.

For two decades, the DSB has maintained steady attention to the health of the U.S. nuclear enterprise, the advances and modernization efforts undertaken by Russia and China, nuclear weapons proliferation to other nation states, and advances in technology that could detect or hide proliferation. DoD leadership is renewing its commitment to the nation's nuclear deterrent, given the relatively recent recognition of the pervasive threat of adversaries' nuclear capabilities and doctrines. The DSB's history in nuclear deterrence helps the Department re-establish a knowledge base, now largely atrophied, to support modernization of our forces and operational readiness to deter nuclear aggression.

In short, "nuclear" still matters, nuclear is in a class of its own, and nuclear cannot be wished away. The nuclear threshold may decrease owing to the stated doctrine and weapons developments of some states, e.g., "escalate to de-escalate," and the introduction of new technology. Further aggravating the situation, the lead time for nuclear modernization and response is *very* long.

3. Preparing for Gray Zone Conflicts

Constrained military operations, short of all-out war, are becoming the norm

As nations have realized they cannot match the U.S. with conventional military might, many adopted strategies and tactics designed to stay below the threshold of a major international armed response; witness Russia in the Crimea, China's island building in the South China Sea, and North Korean provocations. Their tools and techniques include information operations, using disinformation and strategic communication aimed at their populace, neighbors, and the world; ambiguity of forces ("little green men,"

proxies, and naval forces labeled "Coast Guard"); and coercion involving economics, energy, and political corruption. The DSB has identified DoD's options in addressing this "new normal" category of threats and to highlight the role of other parts of the government critical to successfully countering such strategies.

4. Maintaining Information Superiority

What the information infrastructure is enabling—for adversaries and for us

Information has become a decisive and discriminating enabler of modern warfare, and information superiority a potent deterrent. The DSB has published a number of reports highlighting how the DoD can achieve and maintain information superiority, focusing on intelligence collection and analysis, the use of unclassified "big data," and the rapidly advancing technologies of information and communication infrastructures.

The U.S. and its adversaries realize the criticality of information: its assured availability and integrity, and the vulnerabilities in providing it. The DSB advised on offense and defense in this domain, including the growing threats and opportunities in electronic warfare and cyber. As an example, the Board's cyber efforts addressed: matching our defenses to the sophistication of the threats and criticality of the target; managing cyber defense to make optimal use of funding and of scarce technical human resources; determining the challenges and opportunities of cyber relative to new technologies, including cloud computing; identifying strategies to mitigate cyber corruption of the supply chain, particularly foreign supplied microelectronics; and how to deter cyberattacks when defenses are inadequate.

Information remains a critical differentiator for the U.S. and for its adversaries; cyber, cyber corruption of the microelectronics and software supply chain, and electronic warfare offer threats and opportunities vis-a-vis information; and acquiring enabling information technology, particularly software, has its own unique quirks.

5. Anticipating More Intelligent Systems and Autonomy

Numbers and disaggregation
Range
Danger on and above sea surface drive combat undersea

The unmatched capabilities of U.S. joint forces depend on relatively small numbers of extremely capable, high value assets; e.g., the world's most potent aircraft carriers. Predictably, those unique assets became lucrative targets of adversary states, calling into question some foundational operational tenets such as air dominance. DSB's work in this area has advocated ways to operate at greater range from the adversary to increase safety; use of large numbers of inexpensive assets to augment small numbers of costly assets ("quantity has a quality all its own"); and use of carefully managed and controlled autonomous systems to keep Military Service personnel out of harm's way. In addition, capitalizing on U.S. undersea dominance, the DSB has identified ways to maintain that superiority for the near future through the use of large numbers of inexpensive unmanned undersea vehicles to conduct operations that would otherwise be undertaken with greater risk from the air, sea or land.

Intelligent systems, at rest or in motion, will be a differentiator for the U.S. and for its adversaries. The technology lends itself well to disaggregation, numbers, and long range both as an advantage and danger to the nation. Currently, and for the near future, the U.S. owns the undersea domain, where intelligent systems, disaggregation, quantity, and long range can offset the cruise and ballistic missile and the electronic warfare threats to conducting missions from the sea surface and the air.

6. Supporting Stabilization, Reconstruction, Peacekeeping, and Nation Building
Winning the peace

Taking lessons from history, the DSB highlighted the importance of comprehensive planning and preparation before, during, and

after conflict to secure short- and longer-term stability once hostilities cease. The DSB has addressed issues including: identification of the information and intelligence required to conduct stabilization and reconstruction operations successfully; the best use of the National Guard and Reserves with their civilian sector skills; language and cultural training; and campaign planning and exercising for stabilization and reconstruction missions on par with what the Military Services do for combat missions.

Many stabilization, reconstruction, peacekeeping, and nation-building missions are regrettably challenged by insurgency as in Iraq and Afghanistan. While there is no foolproof way to avoid and eliminate insurgency any more than there is a way to avoid and eliminate crime, the DSB has addressed ways to mitigate and manage insurgency to enable the emergence of peaceful societies.

7. Preparing for Surprise
To the U.S. and by the U.S.

The world is an unpredictable place, particularly with the galloping advance of technology. No matter how well the DoD plans and prepares there will be surprises, and there is the ever present value of inflicting surprise on adversaries. The DSB has published reports advising the DoD on how the Department can be better poised to respond to surprise with agility, adaptability, and resilience, e.g., having a technology infrastructure that can be swiftly and inexpensively re-vectored to meet changing needs and threats, using more red teaming and free play in training and exercises. The DSB has also identified potential technological surprises and advised on hedging strategies should those occasions arise.

An agile and responsive acquisition system will enable the U.S. to prepare for surprise, particularly with a requirements regime based on rational analysis of "what to buy" and "how to buy it." This encourages creativity from the scientists and engineers in U.S. industry and universities. The DSB has published a series of reports on acquisition reform meant to underpin a culture of innovation.

In the Board's view, an innovative DoD should introduce change in to the field: new potent systems, creative strategies and tactics, powerful operational concepts, and outstanding Military Service personnel performance at such a dizzying rate than no adversary has hope of developing countermeasures fast enough.

A strong technology base, including knowledge of emerging science and technology, dedicated scientists and engineers, and infrastructure and facilities, acts as a solid foundation in the preparation for surprise. It provides the DoD both strategic differentiators and strategic necessities. The DSB has addressed the need for a healthy technology base in a series of reports, and recommended actions to maintain a U.S. lead in the face of increasing globalization of science and technology.

In sum

The seven chapters that follow point to a blueprint and agenda for the new Administration to enable a fast start in addressing pressing national security issues and opportunities.

CHAPTER ONE

Protecting the Homeland

1. PROTECTING THE HOMELAND

AGAINST NON-STATE ACTORS ▪ *AGAINST ENEMY STATES IN TIME OF WAR* ▪ *AGAINST WEAPONS OF MASS DESTRUCTION AND CYBER*

The DoD's highest priority remains the protection of the homeland, and since 9/11, the nation can no longer consider the homeland as a sanctuary. Even prior to 9/11, the DSB was concerned about the asymmetric evolution of the post-Cold War threat and potential for attacks within the United States. The DSB has focused on clarifying the DoD's roles and assessing its posture for defending the homeland and anticipating these new forms of threats as they become more widespread. Of particular concern is the Department's dependence on critical infrastructure, the supporting capabilities it will need to provide to civil authorities, and shortcomings in the interagency, in broad and more specific contexts, ranging from the violent behavior of individuals to cyber and weapons of mass destruction (WMD) attacks.

9/11 catalyzed the nation to address serious attacks on the homeland—for a while

The decade between the end of the Cold War and 9/11 saw technical advances, most notably in information, biology, and microsystems, which rapidly went into widespread, commercial use. While countless positive outcomes were (and indeed still are) the result, the affordability and availability of the technologies globally also introduced new threats, made more serious by the limited resources in both people and money required to do great harm. A number of events offered warnings; for example,

- The rise of radical terrorist groups as evidenced by the 1993 World Trade Center bombing and Al Qaeda's bombings aimed at U.S. related targets in Yemen, Nairobi and Kenya;

- Aum Shinrikyo's crossing a threshold for terrorist attacks with its sarin release in the Tokyo subway; and

- The Democratic People's Republic of Korea's non-compliance with its obligations under the Nonproliferation Treaty.

The prevailing view in the U.S., however, was that with the Cold War ending and the sanctuary afforded by geography, the nation was safer than it had been in decades.

> **Weapons of mass destruction—nuclear, chemical, and biological—may be accessed by almost any state or non-state actor that desires them more easily than a decade or two ago.**

The events of 9/11 changed that complacency. The following decade saw high profile efforts by the government to address threats to the homeland, focused principally on non-state terrorism and their potential for executing "unconventional" attacks. The DoD's major contribution was "the away game," a decade-plus commitment of military forces in Iraq and Afghanistan to disrupt or destroy adversary networks and enable local government forces to protect their populace. More recently, the nation began pulling back from its military deployments and operations, and rebalanced efforts at the Department of Homeland Security (DHS) to improve emergency response and consequence management for natural disasters. Emphasis related to national security now rests on the rise of provocative actions by nation-states, such as Russia and China, and on the breeding grounds for instability, such as Syria, northern Iraq, and Ukraine. Again the emphasis is on "the away game" roles for the DoD.

Despite the rise of provocations abroad, threats to the homeland must regain attention as a serious concern, as evidenced by the alarming increase in terrorist or terrorist-inspired attacks in Europe, and the incidents at home in San Bernardino, Chattanooga, and Orlando. Overt motives for attacking the U.S. homeland, besides terrorism, include delaying and disrupting global projection of U.S. armed forces to give an adversary time to solidify gains elsewhere, or the mistaken belief that the U.S. can be dissuaded or deterred and its will to fight eroded. More covert motives may be to influence or cast doubts on political agendas, or wreak havoc in financial networks. Adversaries may be "composites" of states and proxies. With advances and availability of key technologies, their means of attack are broader and may vary; and targets have become increasingly interdependent as reliance on information technologies has grown. Weapons of mass destruction—nuclear, chemical, and biological—may be accessed by almost any state or non-state actor that desires them more easily than a decade or two ago.

The DoD's priorities in homeland defense have emphasized taking the fight to the enemy

The events of 9/11 resulted in a shift in the nation's approach to defending the homeland from one that relied principally on offense and assured response to one that added preparedness for dealing with an attack within the borders of the U.S. From the start, the DoD viewed its role in this strategy

as the principal in prosecuting the "away game," confirmed by the military commitment to the prolonged engagements in Afghanistan and Iraq, as well as the legal restrictions of *posse comitatus* and the Insurrection Act of 1807. As such, the DoD has tended to limit its attention and resource commitments to the activities related to homeland defense for which it is directly responsible; e.g., force and installation protection, protection of the defense industrial base infrastructure, special support for domestic nuclear events, NORAD, anti-submarine and anti-surface warfare and patrols, and state-assigned National Guard units.

The most visible and enduring change since 9/11 has been the creation of the U.S. Northern Command (NORTHCOM). This unified a number of command elements in the Department to provide support to civil authorities in those cases where the capabilities of domestic authorities when the local, state, or federal level authorities' capabilities are exceeded, and when directed by the President to do so. NORTHCOM has matured considerably since it was stood up in 2002, both organizationally and in its partnership in the interagency. For example, the improvements by the National Guard, Coast Guard, the U.S. Transportation Command (TRANSCOM) and selected Military Service elements in response to Hurricane Sandy compared to Hurricane Katrina illustrate the responsiveness to lessons learned by both the DoD and the interagency. Through NORTHCOM, the DoD became a major player in interagency exercises and overcame most concerns about its mission to support rather than assume command in a domestic event.

However, in spite of these steps forward, the DSB repeatedly found that the attention to homeland defense is at best episodic when threat levels increase, and priority demands for action and preparedness to engage outside the U.S. overwhelms leadership attention to the problem. As no event as serious as the events of 9/11 have occurred since then, an attitude that "it will not happen here" has returned. Stated more fairly, the risk of another major attack on the homeland has declined significantly in the minds of many.

The DSB has argued that attention to the homeland defense mission must be persistent and engage top leadership in the Department for several reasons. NORTHCOM addresses one major reason, namely the fact that the DoD will be called on to help in the event of a catastrophe that overwhelms civil authorities. However, the Department's preparedness for a widely varying attack menu is not what it needs to be. For example, the DoD appears to have learned important lessons for natural physical disasters with some minimal level of warning, but the Ebola response, in spite of it being principally overseas, highlighted shortcomings for dealing with a biological attack.

A second, "closer to home" reason for the DoD's persistence in attending to the mission is that a major catastrophe will almost certainly affect the Department's ability to prosecute any military action overseas. For example,

- DoD ports or major installations could be a/the target;

- Infrastructure critical to the DoD launching and sustaining an operation, be it the defense industrial base, telecommunications, the electrical grid, and transportation nodes could be targets;

- Cyber attacks most certainly will complicate any preparations stateside for military operations; and

- Some attack modalities, such as biological, will not distinguish civilian from military targets.

The final reason is that technology has moved forward in ways that are simultaneously sophisticated, accessible, and affordable. Schemes of the type orchestrated on 9/11 need not require the same degree of preparation or coordination to do harm on a scale even greater than what we experienced on 9/11.

The DSB recommended that the DoD sustain its involvement with other agencies in improving capabilities and operations within its homeland defense mission responsibilities. The DoD should also plan and operate based on a risk and resiliency

driven paradigm, e.g., to lessen vulnerabilities to single point failures, to remember how to operate in an unconnected world, and to develop and train to less optimal, but robust "Plan Bs."

Individuals—inspired by terrorists—remain a threat

Individuals may seek to disrupt operations or catalyze others to act, despite not likely posing a debilitating threat to civilians or the military using conventional means. In the aftermath of the 2009 Fort Hood shootings, the DSB studied ways to predict violent behavior as one of several DoD initiatives aimed at root causes, lessons learned, or opportunities for avoiding or interdicting such incidents going forward. The DSB's first conclusion was that preventing rather than "predicting" targeted violence should be the Department's goal. While the report did not identify reliable predictive approaches, it did find that good options now exist for mitigating violence by intervening in the progression from violent ideation to violent behavior.

Specifically, professional threat management, as practiced by law enforcement-led threat management units, offers an effective means to help prevent targeted violence. These units are widely used in the private sector and elsewhere in government, but not at the DoD. That should change. In addition, improved information sharing is a vital enabler of effective threat management, and the report also recommended that the Department improve clarity on appropriate sharing of information about worrisome or "red flag" behavior, including developing a collaborative DoD-wide investigative database, with benchmarks to assess progress.

Finally, science and technology initiatives show some promise over the long term as an aid to threat management. The Department should focus on rigorous case studies to aid in the identification of valid behavioral indicators, and should implement and evaluate resilience training. Monitoring of overseas research on screening technologies related to biomarkers should also be pursued.

We must prepare for the worst of attacks

Because the DoD expects to support the U.S. response to a major attack on the homeland, the DSB endeavored to improve understanding and recommend paths to address the worst of them, namely a nuclear or biological attack.

Nuclear Attack. An "unconventional" nuclear attack on the homeland has been a subject of much interest. Initially the fall of the Soviet Union and later instability in Pakistan caused great concern with the "loose nuke" problem. Nation-state proliferation and modernization now garners more attention, and while long-time nuclear powers continue to act in familiar deterrence patterns, proliferators such as the Democratic People's Republic of Korea are not abiding by those norms. Longer-term worries relate to the proliferation of unconventional delivery means (e.g., unmanned platforms and semi-submersibles), and technologies that could enable key steps in weapon acquisition. The DSB has noted the following issues, along with some progress:

- Most of the special nuclear material and weapons reside in the custody of militaries around the world that do not necessarily have the same security principles and practices as the U.S. Programs like the DoD's Cooperative Threat Reduction Program can best mitigate the risk of loss of control; through advancing cooperative monitoring technologies such as the Department of Energy (DOE)'s support of the International Atomic Energy Agency (IAEA); and through military-to-military engagements to build trust and transparency.

- If material or a weapon gets loose and the U.S. has sufficient information to interdict, then the Department will need special capabilities and trained personnel to act. The DoD has made improvements on capabilities and trained operators.

- The initial organization at DHS placed the unconventional nuclear delivery problem among all other research efforts. The DSB's

work highlighted the magnitude of need and gaps in capabilities for detection and response, and influenced the establishment of a dedicated office within DHS, the Domestic Nuclear Detection Office (DNDO), to focus on the "worst of the worst" homeland security problems.

- A major DSB assessment of the nation's ability to provide the earliest possible warning of attempts to acquire special nuclear material or a nuclear weapon indicated a need for revamping the decades-long approach to nuclear activity monitoring. The assessment catalyzed interagency and cross-intelligence community activities to reorient efforts in directions that make use of new data analytics and all-source data management tools.

- For an attack in the making, reliance on radiation detection alone is unlikely to succeed. Sensor and processing architectures that utilize multiple indicators and reach back to suspect behaviors in the early warning ("strategic intelligence") community will be needed.

- The DSB also highlighted the impact of advancing technologies for producing weapons, and with that, the new types of signatures that will need to be monitored for proliferation.

- Studies, programs, and operations associated with the unconventional nuclear problem tend to focus on the pre-detonation phase under the implicit assumption that the U.S. has "lost" if a nuclear weapon is detonated in the homeland. The DSB reminded the DoD and the larger community that it explored many aspects of the post-detonation, "right of boom" phase in the early days of the Cold War. Much of the civil defense guidance to mitigate exposures and consequences remain valid for a limited nuclear attack. The Department can still improve the dispersion models and sensor algorithms to address false alarms, which offer hope for effective consequence management in high population areas, and if in close enough proximity, for detection pre-detonation. The Department continues

to seriously neglect research and development on radiological medical countermeasures.

- If an attack occurs, forensics to identify the source of the material will be critically important. The DSB has highlighted the orphaned nature of some important aspects of DoD capabilities in this area on which the nation is reliant.

Biological Attack. The rapid advances in biotechnology in the 1990s, paired with the revelations of the massive Soviet bio weapons program during the Cold War and evidence of Aum Shinrikyo's aborted efforts to promulgate a biological attack, raised calls from the DSB that the DoD had to pay more attention to potential opportunities and threats in this area. The Defense Advanced Research Projects Agency (DARPA) began investments that have been ongoing since to investigate new medical countermeasures and diagnostics, and detection schemes, especially coupled to control systems for mitigating exposures in enclosed spaces. The anthrax letters followed within a week of the 9/11 attacks and led to a strong push for improved biodefense capabilities domestically. Over the next decade, DHS' flagship program placed detection networks for a limited set of potential agents in major cities. The DoD rebalanced its Chemical and Biological Defense Program to place a greater emphasis on biological threat countermeasures.

The DSB observed that biodefense maintains an innate advantage in that preparedness requires most of the same factors as public health responses to naturally occurring infectious diseases. Concerns about pandemic flu gave impetus to the 2006 national strategy, and more recently, the U.S. under the lead of the Centers for Disease Control (CDC) engaged in the global health security agenda to rapidly detect and respond to an outbreak anywhere in the world. Yet the DSB and other commissioned or independent reports found that a coordinated domestic response system, as recommended consistently, has yet to be realized. This was evident in the numerous initial missteps in the Ebola response; some were across the government, and a number within

the DoD itself, and based largely on confusion about authorities, roles, and responsibilities.

Serious policy and technical issues remain, e.g., recognizing that an attack has indeed occurred; quarantine enforcement; screening the "worried well" at the expense of those more likely exposed; and approved medical countermeasures for all but a few known agents. At a smaller scale, the same problems pertain to the DoD, but it is faced with other complications such as who would have priority in receiving protective gear or treatment should an attack occur within a mixed military-civilian population, and with the fact that mainstream medical professionals in the military are not trained to question symptoms of a disease as anything other than naturally occurring.

The Chemical and Biological Defense Program at the DoD has provided basic protection for military personnel for the threat as the U.S. understood it in the Cold War, but the program has had difficulty keeping up with rapid changes in technology since then, even with DARPA's investments. The DSB believes that the major reason is that commercial pharma and biotech investments have swamped the DoD's investment, such that the Department could be making more progress if it could create a viable partnering arrangement with the private sector. The latest challenge in the biodefense community is the advent of synthetic biology with the implications of gene editing for both beneficial and threatening products.

The new, ubiquitous, and complicating threat is cyber

In almost any scenario, from overseas military operations to physical attacks on the homeland, cyber attacks on infrastructure or military networks should be expected, as the principal or supporting attack mode. In spite of decades of the DSB's and others' warnings to this effect, the DoD largely ignored the possibilities until recently. The U.S. has always enjoyed a formidable offensive capability in cyber operations, but defensive measures have seemed unnecessary or

untenable because of cost or the rapid advances in threat. Chapter 4 of this report covers this topic more thoroughly; but in the context of homeland defense, the tenets of a risk based approach, resiliency to outages or compromises, and fall back options hold even more for cyber than almost any other domain of homeland defense.

Managing risks and achieving resiliency will be key for the DoD in its homeland defense mission

The DoD has taken important, but incomplete, steps since 9/11 to improve its ability to execute the homeland defense mission. Legislative and policy restrictions that cede the lead domestically to other parts of the government complicates progress, but no one questions that the DoD will be a major, if not dominant, player in the event of a catastrophe for which civilian authorities are overwhelmed. In parallel, the DoD must be able to deploy anywhere in the world, while also potentially being the target of attacks on the homeland. Both aspects require a level of vigilance and sustained effort regarding the "home game," on which the DoD does not strongly focus.

Moreover, the advances in the threat that have made potential crises more complex (e.g., "with cyber") or yet more serious (e.g., "with WMD") jeopardizes the progress made since 9/11. While the Department cannot address all imaginable threats and scenarios, it can lead the nation in what it does best in warfighting, namely judging risks and building-in resiliency to planning, capabilities, and operations.

Supporting DSB reports

DoD Responses to Transnational Threats (1997 summer study)

Protecting the Homeland (2000 summer study)

DoD Roles and Missions in Homeland Security (2003 summer study)

Preventing and Defending Against Clandestine Nuclear Attack (2004)

Reducing Vulnerabilities to Weapons of Mass Destruction (2005 summer study)

Deployment of Members of the National Guard and Reserve in the Global War on Terrorism (2007)

Critical Homeland Infrastructure Protection (2007)

Unconventional Operational Concepts and the Homeland (panel report of the 2007 summer study)

Science and Technology Issues of Early Intercept Ballistic Missile Defense Feasibility (2011)

Predicting Violent Behavior (2013)

Deterring, Preventing and Responding to Threat or Use for Weapons of Mass Destruction (final report in process)

Cyber Deterrence (final report in process)

CHAPTER TWO

Deterring the Use of Nuclear Weapons

2. DETERRING THE USE OF NUCLEAR WEAPONS

Despite the "peace dividend" at the end of the Cold War, the DSB remains unconvinced that downplaying the nation's nuclear deterrent would lead other nations to do the same, even as advances in the U.S.' non-nuclear warfighting capabilities proved their effectiveness. In fact, U.S. conventional dominance demonstrated in Bosnia, Iraq, and Afghanistan, as well as regional imperatives, appears to have catalyzed a greater interest in nuclear weapons by others who do not have the resources to overmatch the U.S. otherwise.

The DSB has therefore maintained steady attention on the health of the U.S. nuclear enterprise, Russian and Chinese efforts to advance and modernize, nuclear weapons, proliferation to other nation states, and advances in technology that could both detect and hide proliferation. The collection of findings point to a worrisome conclusion: the nuclear threshold may be decreasing owing to the stated doctrines and weapons developments of some states, and with introduction of new technology. The looming end-of-life of the Triad components and aging production infrastructure forces both the DoD and the DOE to commit substantial resources to nuclear modernization. The lead time for obtaining a modernized force is long and the U.S. is starting well behind Russia and China's efforts.

Even more importantly, the Department must re-establish the knowledge base in nuclear matters and the art of deterrence among both civilian and military leadership, which has largely atrophied.

In short, "nuclear" still matters, nuclear is in a class of its own, and nuclear cannot be wished away.

Nuclear weapons are a steadily evolving threat—in both familiar and new dimensions

The threat from nuclear weapons grew in ways not experienced during the Cold War. Established nuclear powers modernized and expanded their capabilities in both traditional and non-traditional

> **The Department must re-establish the knowledge base in nuclear matters and the art of deterrence among both civilian and military leadership, which has largely atrophied.**

ways. Both China and Russia began modernizing their strategic forces well ahead of the U.S.' commitment to do the same, while also integrating additional elements such as intermediate range missiles, into their force structure. China's nuclear efforts focus on a survivable second strike force, complemented by non-nuclear capabilities that match or offset U.S. non-nuclear forces and networked operations. In addition to its strategic force modernization, Russia embarked on a steady path since the late 1990s of conventional improvements in precision, stealth, and speed, and development and deployment of theater nuclear weapons with a range of tailored effects as a foil to U.S. conventional superiority. Russian doctrine is publicly stated as "escalate to de-escalate" based on the assumption that its first use of low yield nuclear weapons against a conventionally superior NATO force would engender a halt to further aggression.

The Department has seen the relentless pursuit of nuclear capabilities to threaten the homeland by the Democratic People's Republic of Korea, the proliferation of theater weapons in Pakistan, the recently halted march to acquisition by Iran, and the talk of proliferation by some non-nuclear allies and partners who are questioning the U.S.'

commitment to extended deterrence and security guarantees. Commerce in the sale or sharing of nuclear materials and weapons design appeared, and advances in technologies readily accessible even to terrorists introduce new pathways to acquisition.

Nuclear deterrence remains a cornerstone of our national security

Although the threat of nuclear Armageddon has subsided, the nation must still hedge against such an existential possibility, no matter how slim. However, the threats of proliferation, the potential for the U.S. weakening assurance guarantees of its allies, and the emerging scenarios of limited use in regional conflicts or limited strike against the U.S. homeland—with the potential for escalation—introduce complexities not seen since the early days of the Cold War. To address both instances, U.S. policy evolved to seek to raise the threshold for nuclear use, at least by the U.S., by relying less on nuclear forces and more on our advanced non-nuclear capabilities, while also committing to modernizing those nuclear force elements deemed critical for deterrence against a massive exchange. Such complexity called for new reviews of the requirements for a modernized

Triad that includes the weapons themselves and the enterprise for design, production and operations. It also brings to the fore important related topics, such as early warning of proliferation that would allow for rollback options long before a proliferated capability were deployed, and nuclear survivability to ensure credibility of all force elements, nuclear and non-nuclear alike, that the U.S. would like to include in its deterrent arsenal.

Strategic force capabilities. The DSB, as early as 2004 and again in 2006, recommended a shift in U.S. deterrent posture to a broader set of non-nuclear options for strategic strike, and in parallel, research in nuclear weapons to meet emerging needs for ease of manufacture, higher margins, lower collateral damage, and special effects. The near exclusive focus on life extension of existing U.S. nuclear weapons was thought, even at that point, to be limiting flexibility for addressing an uncertain future. With respect to the force mix, the *2010 Nuclear Posture Review* made clear that such a shift to greater reliance on non-nuclear capabilities for strategic deterrence was a priority, but it also called for nuclear modernization while reducing the numbers of deployed weapons. The notion of "cross-domain deterrence," in which non-nuclear capabilities can be readily integrated to meet unique adversary challenges as they present themselves, has emerged as a policy concept. Observing that in the six years since the *2010 Nuclear Posture Review*, there has been little proof testing of the cross-domain proposition, the DSB has outlined a path forward to do so. That path includes red teaming, gaming, and exercising to test the DoD's abilities to integrate and achieve desired effects; much earlier warning to provide many more options in stemming proliferation or escalation; and a more flexible nuclear enterprise that could produce, if needed, a rapid, tailored nuclear option for limited use should existing non-nuclear or nuclear options prove insufficient.

A balanced program to support the nuclear force would consist of three elements for maintaining deterrent force capabilities: (1) certification and maintenance of current systems; (2) life extension of current systems, and replacement of those systems that can no longer be maintained to the required levels of reliability, safety, and security; and (3) a hedging thrust for responding to future uncertainties. For the first two decades after the end of the Cold War, the U.S. remained unbalanced among the three as the DoD laid its attention almost exclusively to sustaining the existing stockpile. Attention to the second element only grew with the "impossible to ignore" reality in the last few years of end-of-life of critical platforms and exhaustion of some warhead replacement components, where the DoD and DOE made substantial commitments of resources to replace, in whole or in part, platforms and warheads.

Yet there is no clearly identifiable set of activities that address the third element, a convincing hedge to future uncertainties, nor has there been since the early 1990s.[1] The DSB has assessed that a robust program should consist of two major components: tailoring of current or planned capabilities and threat anticipation. Regarding the existing or already planned capabilities, efforts should address features such as:

- Enhanced platform survivability;

- Open architectures for upgrades to address technological advances, changing threat environment, and mission confidence;

- Lower yield, primary-only options; and

- Advanced manufacturing to support timely modifications.

Threat anticipation would rely on red teaming

---

1. The DSB observed that there appear to be several reasons, starting with 1993 legislation that forbid the development of new nuclear military capabilities. The legislation was modified later to allow research and development on new capabilities, but any transition to production would require Congressional approval. Both the DoD and DOE, having stopped all exploratory and advanced development with the 1993 legislation, never reversed course after the modification. Congress recently became aware of the situation and purposely included a call for research and development in 2016 authorization language.

informed by trends surfaced through early warning to focus concept and advanced development and prototyping, placing options "on-the-shelf" should they be needed rapidly. Already the DoD can anticipate the need for capabilities such as hardening or maneuvering for defense penetration; command and control to target to allow command disable in flight should a limited strike scenario not evolve as anticipated; real time battle damage assessment; and embedded weapon system state-of-health monitoring. To rapidly field such capabilities would require a production capability utilizing state-of-the-art manufacturing techniques, weapon system architectures, and certification strategies that could support block changes or "plug-and-play" components.

Skills and readiness of the nuclear enterprise. A key contributor to nuclear deterrence is the exercise of the development, design, and production functions for nuclear weapons in the DoD and DOE. The DOE principally manages warhead development and production. The DoD's roles are equally critical in setting system requirements, synchronizing the development, production, and adaptation of the delivery platform, and setting the weapon-platform interface requirements.

The recent uptick in priority for nuclear force modernization in both departments sends a strong message of U.S. commitment to the deterrent, but it comes after 25 years of downplaying (and poorly resourcing) the mission. The question then naturally presents itself as to how quickly the DoD can rebuild the enterprise to a level that matches the demands now placed on it. By enterprise, the Board means the spectrum from research and development, production and test, and operations and maintenance, etc. and the story remains mixed. Some examples include:

- Smaller numbers and types of weapons mean that more resources can be devoted to fundamental understanding and careful monitoring for reliability, but reliance on any one system is much higher and increases the risk of problems or failures that would affect a larger fraction of the force at any one time.

- Underground nuclear testing provided both stockpile confidence and a powerful tool in advancing scientific understanding, but nuclear testing has not been permitted for 25 years. In its place, the nation supported the Stockpile Stewardship Program that significantly improved the fundamental understanding of material aging and nuclear explosive physics through a combination of above ground simulators, and state-of-the-art computational modeling. An open question remains as to how long one can have confidence in the weapons through these approaches alone.

- The DOE laboratories and DoD contractor community did little integrated design and development work outside of life extension for 25 years. They are ramping up their efforts, but of necessity the new workforce contains a large fraction of inexperienced scientists and especially engineers.

- Responsiveness of the DOE complex is low because of a much stronger emphasis on safety and security embedded in Cold War era processes and facilities, some of which date back to the late 1940s. The capacity of the production complex is fully scheduled through the 2040s.

- Plans for facility recapitalization compete with warhead life extension programs and modernization programs. The last successful construction of a new nuclear production facility was in 1976. This becomes especially challenging in nuclear production facilities for plutonium components at Los Alamos and uranium components at Oak Ridge Y-12. Pit production of up to 30 per year is not planned before 2026; production rates beyond that are uncertain.

- The DoD platform modernization requirements are occurring almost simultaneously and extend over two decades. The total budget on the current schedule will significantly compromise investments in conventional capabilities, both new and those that need to be replaced after 15 years of fighting in Iraq and Afghanistan.

Monitoring to achieve early warning of nuclear proliferation should be improved

Another aspect of deterrence has always been limiting the number of nations possessing nuclear weapons (nonproliferation) and of those that do, limiting the numbers in their arsenals (arms control). Renewed interests during the Obama administration in improving the security of nuclear materials globally and advancing arms control agendas with the Russians led to a DSB effort to assess technologies in support of future arms control and nonproliferation treaties and agreements. The DSB realized that any progress in treaties and agreements had to take into account the compounding complexities that appear to be aggravating nuclear proliferation concerns into the foreseeable future:

- Rogue state actions, such as those of the Democratic People's Republic of Korea, and the potential cascading effects on neighboring allies or partners;

- The impact of advancing technologies relevant to nuclear weapons development;

- The growing evidence of networks of cooperation among countries that would otherwise have little reason to do so;

- The implications of U.S. policy that relies more heavily on conventional military superiority as a major element of deterrence, accompanied by reductions in numbers of our nuclear weapons; and

- The wide range of motivations, capabilities, and approaches that each potential proliferator introduces; i.e., it is not just about Russia.

In such a context, the DSB concluded that the technical approach for monitoring cannot continue to derive only from treaty and agreement dictates for "point" compliance to the numbers and types formally agreed upon and geographically bounded. Proliferation in this future context must be a continuous process for which persistent surveillance tailored to the environment of concern is needed. This leads to the need for a paradigm shift in which the boundaries are blurred between monitoring for compliance and monitoring for proliferation, between cooperative and unilateral measures. Monitoring will need to be continuous, adaptive, and frequently tested for its effectiveness against an array of differing, creative, and adaptive proliferators. In order to create such a comprehensive monitoring framework, three key elements would be needed:

- A systems analytical "white team" able to posit alternative futures, assess current capabilities to detect proliferation, identify gaps, and evaluate alternatives;

- New tools to enable proliferation detection as early as possible to achieve persistent monitoring over large and widespread geographies, physical and virtual, along with the data analytic capabilities to sift through the massive data sets generated; and

- A red-blue field testing capability to elucidate the signatures for proliferation involved with small programs, denial and deception, advanced technologies, etc.

Deeper looks into the early warning problem suggest that there is as yet untapped potential in open source monitoring, making use of state-of-the-art techniques in "big data" analytics, for queueing more sophisticated and precise collection resources.

Nuclear survivability is necessary for credible deterrence

It should be obvious that if U.S. nuclear forces are to be part of a credible deterrent, they must be able to survive and function in an adversary generated nuclear environment. What has not been as evident for some time is the parallel need for critical non-nuclear forces to be able to "fight through" in a nuclear environment if indeed the U.S. seeks to rely more heavily on those forces as part of its deterrent posture. In both cases the attention paid to the topic of nuclear survivability

remains limited, in part because of perceptions that the only recourse is equipment hardening and that cost to harden is prohibitive, and in part because of the atrophy in the specialized knowledge in nuclear weapons effects and warfighting principles associated with survivability.

The DSB's persistence on this topic from 2005 to 2015 produced a series of reports that can be summarized as follows:

- A consequence of the reduction in numbers of U.S. nuclear weapons is that an even higher premium is placed on reliability and survivability of the remaining force, especially in the limited use scenarios imagined for the future.

- Expertise in the Combatant Commands to assess and plan for U.S. conventional force operations in an adversary generated, limited nuclear environment is lacking, and the survivability of countless force elements is not known.

- General knowledge in the military regarding nuclear weapons and the environments they generate, outside of some in the strategic force cadres in the Air Force and Navy and a small group of specialists in the Army, does not exist. The Defense Threat Reduction Agency (DTRA), the Military Service laboratories, and specialized commands, national laboratories, and contractor communities, along with aboveground test facilities hold small pockets of technical expertise in nuclear weapons effects.

- The evolution of the conventional forces to systems that depend on commercial suppliers, the introduction of increasing levels of autonomy, and the reliance on networked operations are producing a potentially more vulnerable force, but we do not know to what degree.

- The Department is making several major acquisitions as it modernizes the nuclear force and introduces new offset capabilities. These systems will be with the DoD for a long time to come, so that the Department should be buying all the survivability it can afford as a hedge against an uncertain future.

- "Buying survivability" does not necessarily equate to hardening. The Department can relearn many lessons from the Cold War in which tactics, redundancy, and recovery were viable options for "fighting through." Moreover, the cost to harden already fielded systems is indeed likely to be prohibitive, such that alternative approaches will be important for addressing legacy systems.

The significant change required to re-create nuclear literacy in the DoD will take leadership from the top. While some noticeable and noteworthy efforts are underway, progress will necessarily be slow to develop a new generation of nuclear savvy acquirers, planners, and operators. The DSB recommended that starting with a focus on mission assurance could lead to affordable and timely decisions and planning. It will require a concerted effort, with the following characteristics:

- Combatant Commands should identify mission critical functions derived from operational plans and Military Services then devolve that to mission critical capabilities;

- The analytical community should provide support to link mission critical capabilities to specific systems and tactics;

- The operational community should conduct gaming and experimentation in radiation degraded environments to identify gaps and uncertainties;

- The Military Services should ensure a tiered system of education and training in nuclear warfighting, including a basic level of knowledge throughout the force and among decision makers;

- In filling gaps, the acquisition community should set requirements and the testing and evaluation community conduct assessments tied to mission assurance, not simply hardening levels; and

- The technical community should support all of these activities.

> The nation and the Department are stepping up to the commitment needed, but the price to pay in both human resources and budget is substantial, given the two-plus decades of neglect.

The DSB strongly recommends that all major acquisitions be born with a nuclear survivability requirement derived from projected threat scenarios relevant to the range of missions expected for the system.

U.S. nuclear modernization has been put off too long

The level of interest in nuclear weapons has grown with existing nuclear powers, who are modernizing their forces, and in some cases, expanding their capabilities both qualitatively and quantitatively, and with new or latent proliferators. Principal drivers include an affordable hedge against U.S. conventional superiority and a deterrent against regional actors that threaten their interests or sovereignty. In parallel, an aging nuclear force and enterprise to support it in the U.S. has forced the need for a modernization program of our own. The nation and the Department are stepping up to the commitment needed, but the price to pay in both human resources and budget is substantial, given the more than two decades of neglect. Through its persistence over those decades, the DSB produced a compendium of findings and recommendations that can provide a rapid head start for the re-learning that must take place.

Supporting DSB reports

Future Strategic Strike Forces (2003 summer study)

Employment of the National Ignition Facility (2004)

Nuclear Weapons Effects Test, Evaluation, and Simulation (2005)

Nuclear Capabilities (2006)

Nuclear Deterrence Skills (2008)

Report on the Unauthorized Movement of Nuclear Weapons (2008)

Nuclear Weapons Inspections for the Strategic Nuclear Force (2008)

Nuclear Weapons Effects National Enterprise (2010)

Independent Assessment of the Air Force Nuclear Enterprise (2011)

Air Force Nuclear Enterprise Follow-On Review (2013)

Survivability of Systems and Assets to Electromagnetic Pulse (EMP) and other Nuclear Weapon Effects (5 reports, 2011–2015)

Assessment of Nuclear Monitoring and Verification Technologies (2014)

CHAPTER THREE

Preparing for Gray Zone Conflicts

3. PREPARING FOR GRAY ZONE CONFLICTS

CONSTRAINED MILITARY OPERATIONS, SHORT OF ALL-OUT WAR, BECAME THE NORM

Adversaries have been able to blunt the effectiveness of U.S. military power by pursuing sophisticated but lower risk approaches to challenge to U.S. security interests without triggering a major U.S. military response—in spite of the profound effectiveness of U.S. military power in place at the end of the Cold War. In several important cases, nations sought to deter U.S. military intervention by creating powerful area denial and anti-access capabilities, including nuclear weapons and flexible doctrines governing their employment.

Since the end of the Cold War, the confrontation and competition for influence usually takes place below the threshold of major inter-state armed conflict. The strong and the weak, developed and undeveloped nations, near peers and rag-tag nations, and even self-proclaimed non-nation states challenge and confront each other to improve their relative position—politically, militarily, economically, or to increase influence among a population.

Illustrative of these adversary campaigns in Europe include Russia's gray zone efforts between war and peace to compel the independent states of the former Soviet Union to join a Russian led "Eurasian" entity. In East Asia, China's efforts to convert the exclusive economic zone aspects of the Law of the Sea Convention into a sovereignty claim over the entire South China Sea enforced by its militarized "Coast Guard" to enforce it without incurring the risk of a U.S. military response has, so far, been proceeding.

Such competitions are typically open to multiple interpretations and U.S. interests are not clear. The Department could conduct actions at low "cost" i.e., low risk to U.S. lives, low risk to high value U.S. military assets, little danger to innocents, and little damage to infrastructure, as the U.S. may have to rebuild it later. Public opinion strongly shapes the rules of engagement: global public opinion, U.S. public opinion, public opinion of an ally, and public opinion of the adversary.

These conflicts take many forms; the conflicts offer no clear line between peace and war may go on for years at widely varying levels of intensity below the threshold of an international response, particularly in the absence of a U.S. decision to escalate. The U.S. may need assistance from other nations for transit and access and to shape public opinion. Some confrontations, which tend to be regional, involve an insurgency acting against a standing government, military, and political activities within a sovereign nation conducted by a neighbor, disputes over territory between neighboring nations, campaigns to undermine or enhance cultural influence, or terrorist or criminal activities within states or ungoverned territories.

Some challenges involve neither territorial domination, nor forceful confrontation, but still intended to advance adversary interests and frustrate U.S. efforts to protect its own interests. For example, these may involve theft of intellectual property, maritime displays of sovereign presence, media campaigns to wrongfully discredit U.S. soldiers in foreign locations, release of information stolen digitally, and penetrating a component supplier in order to degrade the performance of the weapon system in which the component is embedded.

The cumulative effect of these developments is the global attrition of U.S. power and influence, and a diminished U.S. will and a lack of a guiding strategy to affect events. Further, the success of such gray zone tactics stimulates other nations who share little else apart from their antipathy to the U.S., its allies, and the interests they share.

The U.S. has responded to gray zone confrontations in the past

The U.S. responded to a somewhat similar diminution of influence and power in the middle of the last century just after the end of World War II. In just four years of post-war gray zone operations, the Soviet Union succeeded in imposing Communist regimes that enveloped much of Central and Eastern Europe as well as China, the Democratic People's Republic of Korea, and

eventually most of Indochina—underpinned by the Red Army and the future prospect of the Soviet Union as a nuclear power competitive with the U.S.

The relentless expansion of territory under the control of the Sino-Soviet alliance in the years immediately following the end of World War II exploited the near-abandonment of the U.S. forward military posture as it demobilized in the European and Pacific theaters of the conflict. The U.S. briefly held a nuclear monopoly: in 1949, the Soviet Union detonated an exact copy of the U.S. weapon used at Nagasaki four years earlier. The U.S. nuclear posture during its period of holding a nuclear monopoly was diplomatically and politically inconsequential in enforcing the 1945 Yalta and Potsdam agreements.

In 1950, the U.S. leadership came to recognize the cumulative toll exacted by these undeterred gray zone operations. Using the newly created statutory National Security Council system, President Truman promulgated the core foreign policy document of the Cold War that shaped U.S. foreign policy until the Soviet Union collapsed in 1991—NSC-68. This document committed the U.S. to a "whole-of-government" approach to confronting Soviet military power that would bring to bear the full weight of U.S. economic and military power to support and sustain a global foreign policy to contain and deter the Soviet Union to the point that it collapsed.

NSC-68 called for substantial expansion and modernization of the military leveraging the technologies of information and precision navigation to field a force capable of persistent surveillance and precision strike that served as overmatch to the capabilities of any other nation. NSC-68 directed the development of a hydrogen bomb and a nuclear force that was able to deter (and extend the deterrent to U.S. allies) any nuclear adversary or coalition of adversaries. NSC-68 called for increased military aid to allies of the U.S., and made containment of global Communist expansion a high priority.

That sustained execution of a whole-of-government response was profoundly successful. It is an appropriate approach for today.

The U.S. must respond to a new form of war

1. **Create an overarching strategic concept:** As discovered in the Cold War, the U.S. needs an overarching strategic concept to enable the whole of government to be effectively mobilized around a national purpose. The U.S. requires a 21st century counterpart to the policy embodied in NSC-68 that will bring together the capabilities of all agencies whose capabilities and resources can favorably affect national security outcomes. Appropriately, a single agency within the national security infrastructure took the lead in drafting such a policy initiative for the President's consideration; in 1950 the Department of State took the lead due to its extensive involvement in post-war reconstruction in Europe and Asia. Today, the DoD's global involvement and capabilities in the management of multiple political-military crises has created a level of expertise unrivaled in the Federal government. Only DoD holds the insight and prowess to address incursion in the information spaces.

2. **Recognize and plan for information needs in Constrained Military Operations:** The gray zone remains a critical battlespace with information needs that differ fundamentally from other types of conflict. These needs include information content and messaging, diplomatic activities, physical assets and activities, and economic activities. All elements affect the information dimension of U.S. activities in constrained military operations.

3. **Broadly shape intelligence strategies and priorities to meet the needs of 21st century conflict while denying adversary access:** While traditional intelligence collection disciplines (human intelligence, signals intelligence, etc.) remain important, the vast array of persistent, universal, and global "open source" intelligence collection can be used to gain deep insights into adversary aims, behavior, and vulnerabilities. Cyber operations, electronic warfare, deception, and kinetic operations can contribute to our ability to deny the adversary access to information and resources.

4. **Increase the use of open source information:** Open source information can contribute significantly to situational awareness, and increase the effectiveness of traditional intelligence collection. It is the result of the observations, thoughts and digital actions taken by multitudes; it is more diverse and derives from more locations than that which the necessarily limited sensors and collectors of the U.S. and its allies collect. It is available on a continuous rather than episodic basis, and can be used to cue other means of information collection, enhancing traditional indications and warning as well as battle damage assessment. The ability to use modern data analytics, including autonomous processing and machine learning, can significantly enhance insights into adversary behavior and to contribute to the U.S. ability to mitigate adversary information operations and deception. The exploitation of highly automated advanced analytic technologies can enable a "deep" understanding of the adversary's culture; politics; influence mechanisms; the commercial, financial, industrial, and governmental infrastructure; core interests of adversary leadership elites; and its vulnerabilities.

5. **Develop and increase the stockpile of tools adapted to serve constrained military operations:** Special Operations forces are committed to constrained military operations today, and are highly effective. The DSB advises increasing that force, using it more selectively, and using it in higher advantage situations. The U.S. could use better and more cyber options. The DoD's provision of arms would be helped if given with means of assuring that they would not be used against the U.S. later. Other useful tools to be developed include: additional techniques for influencing ground movement of adversaries and neutrals; low "cost" no fly zone; low "cost" naval blockade; low "cost" land blockade; much better information operations and the use of social media; weapons

Strategic communication is a dynamic process with responsibility held by those at the highest levels of government—the President and senior government leaders. It must be executed with shared knowledge and strong, adaptive networks within government and between government and civil society.

that are non-lethal and reversible; and better indirect, but compelling, influence on players, e.g. a particular tribe or clan, who could take action in our favor, but are not doing so.

6. **Develop expanded opportunities for deterrence:** The U.S. must deter adversary use of capabilities for which cost-effective defenses are not available. Doing so in turn requires that the U.S. develop a sophisticated knowledge of decision makers, vulnerabilities, their most fundamental interests, and technologies, tactics, techniques, and procedures by which we can hold them at risk.

7. **Engage allied and friendly nations with shared interests to contribute significantly to constrained military operations:** Sharing important capabilities with allies can enhance the effectiveness by which U.S. capabilities apply. Precedents developed during the course of collaboration with allies in counter-terrorism intelligence, diplomacy, implementation of sanctions, and cyber operations well beyond the scope of traditional combined military operations is achievable and effective. Friendly nations can take actions that do not escalate a

confrontation, while if the U.S. took the same action might trigger an unwanted escalation.

Lessons are taught but not learned

The DSB studied the evolving character of post-Cold War military challenges to U.S. interests in several reports prior to the 2016 study for *Constrained Military Operations*. In its 2004 report on *Transition to and from Hostilities,* the DSB noted a recurring pattern embedded in post-Cold War experience. U.S. forces deployed on average once every three years, but while major U.S. military engagements remained very brief (in part due to the superiority of U.S. general-purpose forces), U.S. political-military involvement typically lasted for approximately eight years. Clearly the U.S. needed a better process, both to prepare for future conflicts it could not now anticipate, and a more efficient process of post conflict stabilization. The latter point gave rise to a separate, but related effort concerning stabilization operations in the 2005 report on *Institutionalizing Stabilization Operations in the DoD.*

Repeatedly, the DSB found that U.S. effectiveness was diminished by the absence of effective "strategic communications" as a "lesson taught but

not learned" over several post-Cold War military operations. As stated in *Strategic Communication (2008),* strategic communication is a dynamic process with responsibility held by those at the highest levels of government—the President and senior government leaders. It must be executed with shared knowledge and strong, adaptive networks within government and between government and civil society. Effective strategic communications could in many cases advance U.S. political-military and diplomatic aims more effectively than could military operations.

Supporting DSB reports

Transition to and from Hostilities (2004)

Strategic Communication (2004)

Institutionalizing Stability Operations within DoD (2005)

Strategic Communication (2007 summer study)

Constrained Military Operations (final report in process)

CHAPTER FOUR

Maintaining Information Superiority

4. MAINTAINING INFORMATION SUPERIORITY

The U.S. maintains its global military dominance in large part by innovatively and extensively utilizing information technology in all aspects of warfighting. Unfortunately, the DoD's comprehensive dependence upon this vulnerable technology created unacceptable levels of doubt in the resilience of these systems and thus, in the U.S.' military dominance against an adversary who can hold these systems at risk.

The DSB first highlighted this issue in a report entitled, *Security Controls for Computer Systems (1970)*. This occurred during the transition from batch oriented stand-alone and air-gapped systems to time-sharing distributed systems. This transition opened a Pandora's Box of new security concerns and attack vectors available to compromise computing systems.

During the intervening decades, DoD and society as a whole continued to increase the mission-critical roles and associated dependencies of this rapidly evolving technology. The combination of extensive dependence, high vulnerability, and major consequences of failure turned many DoD systems, both enterprise and mission, into very attractive adversary targets.

Because information has become a decisive and discriminating enabler of modern warfare and information superiority a potent deterrent, DSB increased its efforts in examining challenges and opportunities for achieving and maintaining information superiority. The Board has evaluated intelligence collection and analysis, big data, cloud computing, information and communications infrastructure, interoperability, geo-positioning, and advanced weapons systems while at the same time recommended ways to protect and defend these capabilities. This combination will increase and ensure the U.S.' advantages and at the same time, increase the uncertainty of U.S. opponents.

Today, the U.S.' peer and near-peer adversaries increasingly maintain the ability to hold both U.S.
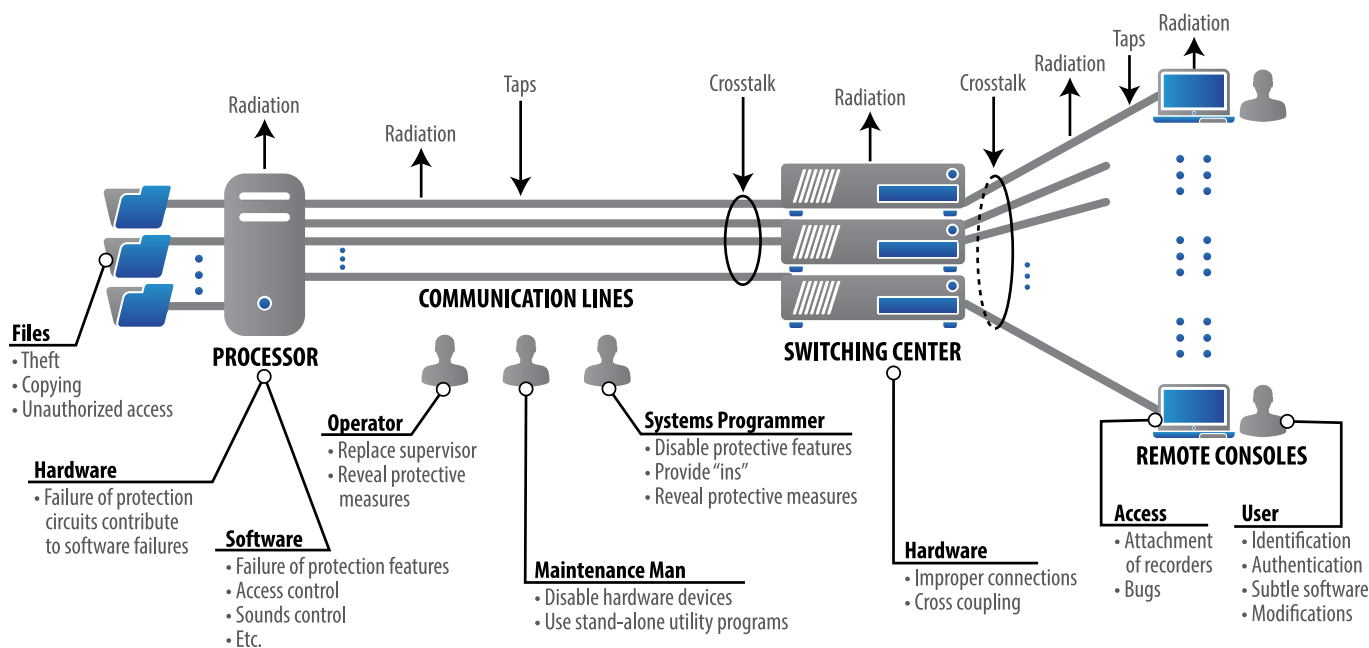
An early analysis of computer network vulnerabilities. These findings were effectively dismissed by many in the defense community at the time, and even for those that understood the significance, very little was done. (DSB Report on *Security Controls for Computer Systems, 1970*)

critical infrastructure and military systems at risk by compromising their information technology underpinnings. Many others have the ability to cause lesser but still grave harm to U.S. information systems. While awareness of this problem is high, progress to decrease the risk remains very limited. In many cases, the trade-space between system function, performance, and security has been too difficult to address. This impasse must be resolved and the DoD must step up its defensive game *now*.

Information superiority is challenging in a complex electromagnetic environment

A central element of information superiority for the United States has been our military's electronic warfare capabilities that are common to most mission areas: tactical communications; satellite communications; positioning, navigation, and timing; and intelligence, surveillance and reconnaissance. The limited availability of high-end electronics to defense system developers in a few large countries in part assured U.S. superiority in electronic warfare. Now that advanced and capable electronics are inexpensively available worldwide,

the U.S.' dominance has eroded and both large and small actors are developing effective electronic warfare capabilities. Without exception, the ability to perform required functions and conduct required operations seriously lacked in all but relatively benign electromagnetic spectrum environments.

The expectation that U.S. forces will prevail in a conflict is predicated to a large extent on information supremacy, especially in an era of network-centric warfare. However, this supremacy will be lost if adversary electronic warfare capabilities deny U.S. forces the ability to sense, communicate, navigate, and synchronize on the battlefield. The proliferation of digital, software-driven electronics provides a technical foundation for very rapid adaption. This translates into a potential ability to change waveforms, techniques, and algorithms for large systems in hours or days, rather than today's normal cycle of years. Certain potential adversaries of the U.S. have much of that capability today and more will acquire it as modern electronics and software continues to be global commodities.

To mitigate the most critical deficiencies, the DSB recommends:

- Managing the use of the electromagnetic spectrum far better and more dynamically than today;

- Adapting to related events, either in terms of mitigating problems or taking advantage of opportunities, far faster than can currently be done; and

- Shift more to offense, because responding to every problem defensively will never get ahead of the adversary, and bound to be unaffordable.

- A final recommendation to revitalize the DoD electronic warfare enterprise was immediately adopted by the DoD, because without appropriate advocacy, oversight, coordination, and supporting infrastructure for EW, any technical improvements will be short lived.

Space and the global positioning system play a central role

The combination of electronic warfare and cyber threats appears daunting. As these historically distinct disciplines increase their level of collaboration, the defensive challenges will increase geometrically.

An excellent example of a foundational technology and platform underpinning the U.S. military's information superiority is the Global Positioning System (GPS). GPS signals permit simultaneous determination of both precise three-dimensional position and precise time and thus, provide a common thread of precise position and time throughout our national security and economic infrastructures. For these reasons, the DSB published its report on the *Future of the Global Positioning System (2005)*. By many measures the GPS appears to be a successful program, however, the report revealed a number of serious issues that affect its operational viability in military effectiveness, civil performance, competitiveness, and governance.

While there has been a growing awareness to which GPS is integral to mission success, there has been insufficient planning or implementation of the changes needed to make GPS more able to support future missions and architectures. The ability of the U.S.' military to maintain GPS service to U.S. forces in the presence of hostile forces remains essential. However, inexpensive, capable, low-power jammers proliferated in the international arms market to deny this service. Potential enemies are undoubtedly aware of GPS effectiveness, and will take advantage of this jammer technology in future conflicts. It is imperative therefore that anti-jam margins for military GPS equipment be raised in order to mitigate the effect of these low power jammers. Additionally, the potential growth in the use of proliferated ultra-wideband networking and communications devices and its effect on the noise floor will likely make consistent reception of all GPS signals more challenging, particularly in metropolitan areas. The DoD understands anti-jam solutions but implementation lags need. The Department should also accelerate the GPS-III programs, and undertake research to further improve the robustness of GPS and explore alternatives to supplement GPS for military positioning and navigation.

The DSB has long held that space superiority is essential in achieving global awareness, information dominance on the battlefield, deterrence of potential conflict, and superior combat effectiveness of our forces. Shortfalls within existing and planned space systems will affect the U.S.' vulnerability to emerging electronic warfare, kinetic, and cyber threats. For critical systems, it is not enough to be resilient to each of these threat vectors; they must be resilient to any combination of these offensive capabilities. The DoD needs strategies to enhance the resilience of the space enterprise, including those critical elements provided by international partners and the commercial sector.

Military microelectronic and software systems must be protected

In large part, rapid improvements in fundamental microelectronic technology, such as those led by Moore's Law, in the past drove the enhancing of the U.S.' information dominance

over all potential opponents. The exponential improvements in hardware such as integrated circuits, microprocessors, microcontrollers, digital signal processors, and programmable logic arrays, led to performance advances in communications, networking, and software. Thus, microelectronics hardware is foundational to U.S. information dominance and the Department must protect it. In *High Performance Microchip Supply (2005),* the DSB noted that the DoD remains highly dependent upon this technology to maintain military superiority—not only information superiority—that the U.S. must maintain a trusted and assured supply of these integrated circuits.

Key potential opponents increasingly engage in the life cycle of this technology: product definition, design, process development, mask making, chip fabrication, assembly, test, customer support, materials, production equipment, and contracting. This causes enormous challenges in the associated supply-chain. The report concluded, "If the real and potential adversaries' ability to subvert U.S. microelectronics components is not reversed or technically mitigated, our adversaries will gain enormous asymmetric advantages that could possibly put U.S. force projection at risk."

The acquisition cycle of a weapon system and the larger life cycle of these systems, provide opponents increasing opportunities to insert exploitable constructs into U.S. systems. The combination of the hardware and software supply chain challenges seems intractable. Even though the level of awareness of these issues grew and new DoD policy and structure developed, the Department remains at great risk. The DSB began a study on the *Cyber Supply Chain (final report in process)* in 2015. The members found that assuring the integrity of weapons systems supply chain has become more difficult (rather than less) and required ever increasing vigilance and sophistication in both acquisition and sustainment. This is due in part to increased globalization and decreased control over suppliers, increased complexity, latent vulnerabilities, and subsequent system modification. Given the unavoidable dependence of DoD cyber supply

chains on commercial components, globally produced microelectronics, and embedded software, and the growing body of evidence that U.S. adversaries exploit the opportunities, the DoD still finds itself extremely vulnerable with inadequate program protection practices and immature technologies to mitigate the risks.

Similarly, and again predictably in *Mission Impact of Foreign Influence on DoD Software (2007),* the DSB observed that the DoD missions strongly depend on software with increasing offshore provenance. While critical military applications were likely develop using trusted or cleared contractors, the lower level software structures such as operating systems could easily have foreign fingerprints. Further, because of the high degree of interconnectedness, should an adversary penetrate any point, the infiltrator can move laterally to other connected systems. This presents a tempting target and may be an inexpensive approach when compared to microelectronics. Once the adversary introduces the malicious code, it would be difficult to detect and could grant access to the DoD system for purposes of denying service, stealing information, or corrupting critical data. Even if the malware were discovered, attribution and intent would be difficult to prove. This ensures a small risk and large benefit for the attacker.

Defense acquisition of information technology is more difficult than ever

In response to a growing concern from the U.S. Congress and among Department of Defense leadership that the nation's military advantage may be eroding, DSB undertook a policy review in its report *Department of Defense Policies and Procedures for the Acquisition of Information Technology (2009).* The scope of the report touches on acquisition oversight policies and procedures, roles and responsibilities for acquisition activity department-wide, reporting requirements, and testing. Importantly, the report found that the deliberate process through which weapon systems and information technology acquired by the DoD cannot keep pace with the speed of introduction of new capabilities in today's information age. Both the length of

time for acquiring new information technology and the openness of the acquisition community allows an adversary provide ample opportunity to develop countermeasures to DoD systems and allows adversaries to leverage U.S. military innovations and employ those same capabilities against the nation. The DoD may need a separate acquisition system for information technology than that used for major weapons systems.

Resilient and effective cyber protection will require a systems approach

Under pressure to increase information sharing and assured interoperability, the DSB published a report entitled *Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise (2009).* The report considered net-centricity a key enabler for information sharing. The overarching national security vision created an assured joint DoD and interagency interoperable net-centric enterprise along with integration with the existing cyber strategy that could enable U.S. decision superiority at all levels. While clearly this would significantly enhance U.S. military advantage, it was not clear how to do this in a cyber-contested environment. The U.S. must temper its appetite for enhanced system performance, functionality, and interoperability with its ability to sufficiently protect these systems from the adversary. This appears straightforward for small insurgent groups, but not as simple for a nation state.

By 2011, a confluence of events and activity markedly increased the urgency and visibility of fully leveraging new information technology developments and at the same time ensuring the resiliency of them. The digital cloud was becoming omnipresent, and seen as the next major step in the evolution of computing infrastructure. The allure and affordability of petaflops of processing capacity, petabytes of data storage, and very high bandwidth became irresistible. At the same time, the Department saw a clear and unambiguous increase in adversary cyber penetrations of the DoD's unclassified and classified networks.

The DSB concluded in *Cyber Security and Reliability in a Digital Cloud (2013),* that against low level opponents and for less critical systems, the cloud held the promise of improved security. Cloud storage provides much better security consistency and a more rapid application of patches. The combination of the security boost and the potential for large cost savings appeared attractive and reasonable for non-critical systems. However, higher tier opponents will likely target the use of cloud technology for critical systems.

One cannot address the resiliency of a system without indicating the level of threat targeting the system. The *Resilient Military Systems and the Advanced Cyber Threat (2013)* report introduced a structure for characterizing various levels of threat. The low-level attacker primarily exploits known vulnerabilities with openly available tools. The mid-level opponent holds the added ability to discover new vulnerabilities and develop the corresponding tool set. Finally, the top-level adversary can also create and operationally introduce supply chain vulnerabilities into their target and perhaps do this at significant scale.

Against this backdrop, the study concluded that the U.S. cannot be confident that critical information technology systems will work under a full-spectrum attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with its entire military and intelligence capabilities. Because risk is a function of threat, vulnerability, and consequence of compromise, to effectively manage risk, the DoD must work the risk reduction challenge as a systems problem.

The DoD must protect the information enterprise

While the DoD's space-based systems and their ground-based support remain critical to U.S. information superiority, they represent just a part of the information enterprise upon which the U.S. military became dependent. Today's military operating environment is increasingly complex. Our adversaries appear dispersed, often mixed with
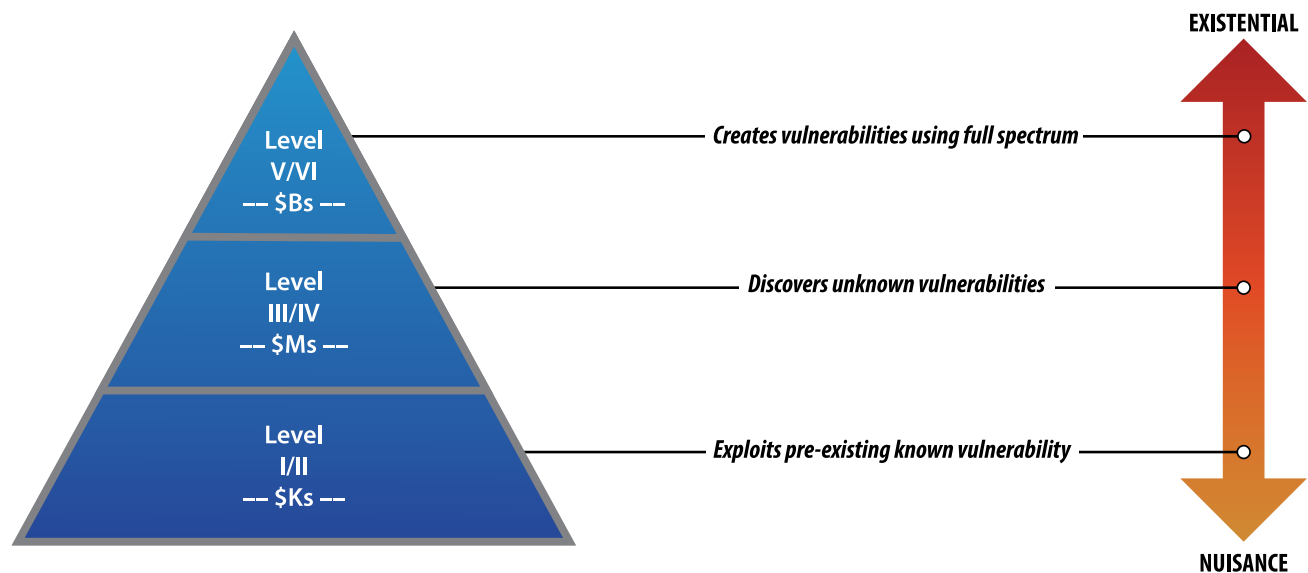
A cyber threat taxonomy proposed in the DSB Report on *Resilient Military Systems and the Advanced Cyber Threat, 2013*

civilians and other non-combatants, and targets located in areas where great concern exists over collateral damage and unintended consequences. Adversaries are adaptive, amorphous, and stealthy, further increasing U.S. reliance on information.

The DSB assessed the department's strategy, scope, and progress toward achieving a robust and adaptive net-centric DoD information management system. The many facets of the problem include support for combat operations, information management, information assurance, and architecture requirements; the DSB found that these considerations converge on the simple question of how to provide robust, useful information at all levels from decision-makers to tactical users.

The DSB evaluated information management in four operational scenarios in *Information Management for Net-Centric Operations (2006):*

- Preventing and protecting the United States against catastrophic attack;

- Conducting large-scale counter-insurgency operations, including stabilization and reconstruction;

- Conducting global distributed, small-scale operations, including counter-terrorism and humanitarian relief; and

- Enabling large-scale operations against near peer adversaries.

Consistently, the DSB's reports found the provocative notion that the DoD's information networks, as a whole, are a critical weapon system and must be protected and operated in a manner consistent with the mission of protecting and defending the United States.

The mission assurance dependencies on DoD networks hold major implications for commanders, operators, and training regimens. A critical defense weapon system requires enterprise-wide operational management, performance monitoring, and contingency planning functions. Operators must know how to operate the combat weapon system, and readiness assessments, throughput and performance, and trades and metrics to measure performance and assurance must be available. Many defense assets connect via this system and system services must be prioritized and tested, and war fighters must train with the system.

The DSB recently investigated ways to improve the overall management processes to provide the needed security to its systems and networks. In *Cyber Defense (2016)*, DSB examined methods to assess and provide leadership with improved cyber protection management, methods to assess

system resilience, and ways to inform future security investments and provide a prioritized list of how to spend its next cyber defense dollar. The combination of very effective red teams and increased adversarial activity significantly enhanced senior leadership awareness and concern, reflected in several "cyber awakening" activities.

Specific and actionable recommendations that collectively aim at significantly augmenting the DoD's defensive position include: collecting and analyzing attack data, engaging senior leadership, automating network management operations, identifying and protecting mission critical systems, including cyber preparedness in defense readiness reporting, developing modeling efforts to inform future investments, and working with commercial suppliers to enhance the security of their products. However, even with these improvements, the DSB recognized that against a top tier opponent these efforts would likely prove inadequate to safeguard the DoD's most vital systems.

A common theme throughout the DSB's numerous evaluations of information superiority is the recognition that the U.S.' information systems will be constantly under attack by its adversaries and these systems must work in a degraded mode. Combat information capacity is no different than any other defense weapons system. As well, doctrine, concepts of operations, tactics, techniques, and procedures, and contingency plans must be developed to address these threats against combat information systems. Relevant systems must be exercised regularly to enable U.S. commanders to understand how to operate in degraded modes. The DSB also addressed organizational roles and strategy to deal with the DoD's increasing adherence to net-centric doctrine.

Because of the inability to sufficiently protect these critical systems in the face of a top tier opponent, the report concluded that the U.S. cyber defensive strategy must include an element of deterrence. This deterrence conclusion resulted in a new study, found in *Cyber Deterrence (final report in process)*. The findings of this task force supported the resiliency report and extended its insights. In particular, the study recognized that due in part to the uncertainty about the offensive cyber capabilities and intentions of potential adversaries, the extent of U.S. vulnerabilities, and the time to recover from an attack even experts disagree whether the potential impacts of cyber-attacks should be characterized as "catastrophic" or "existential." Regardless of this distinction, the offensive cyber capabilities of U.S. adversaries will likely to continue to grow more rapidly than the DoD's ability to defend and make resilient its critical infrastructures. Consequently, the U.S. must prioritize developing and sustaining a credible cyber deterrence posture.

An effective deterrence strategy will tailor the approach for each potential opponent, realizing that people are deterred, rather than nations. As such, the DoD must understand by country and leadership what they hold dear that may be at risk using cyber resilient capabilities. Specifically, kinetic and offensive cyber response capabilities used by the DoD must not only be resilient to traditional attack vectors but also must be resilient to a top tier offensive cyber attack. The innovative use of offensive cyber capabilities to support defensive objectives remains critical to increasing U.S. confidence in its response capabilities and decreasing the confidence of the attacker in their ability to neutralize these response capabilities.

Information technology routinely delivers advantages and vulnerabilities

The DoD uses network connectivity and the integration of state-of-the-art commercial microelectronics and software in both enterprise systems and weapon systems to tremendous advantage, economically and militarily. Unfortunately, this is a double edged sword. The growing vulnerability of these systems to a knowledgeable and motivated adversary keen on reducing U.S. advantages offset these game-changing advantages. It is increasingly clear that this is core to their strategy. As a result, the DoD should expect full-spectrum cyber to be a part of all future conflicts, especially against near-peer opponents. The DSB suggests a strategy to leverage the military utility of this

technology and at the same time sufficiently protect it from our potential adversaries. Cyber remains a complicated domain and requires management from a systems perspective. There is no silver bullet today and there will not likely to be one in the future. While the Department cannot eliminate risks, it must manage risks through a combination of improved cyber defense, a proactive cyber offense to support the DoD's defensive needs, and effective deterrence.

Supporting DSB reports

Future of the Global Positioning System (2005)

High Performance Microchip Supply (2005)

Information Management for Net-Centric Operations (2006 summer study)

Mission Impact of Foreign Influence on DoD Software (2007)

Department of Defense Policies and Procedures for the Acquisition of Information Technology (2009)

Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise (2009)

21st Century Military Operations in a Complex Electromagnetic Environment (2013 summer study)

Resilient Military Systems and the Advanced Cyber Threat (2013)

Cyber Security and Reliability in a Digital Cloud (2013)

Cyber Defense (2016)

Cyber Supply Chain (final report in process)

Defense Strategies for Ensuring the Resilience of National Space Capabilities (final report in process)

Cyber Deterrence (final report in process)

Military Satellite Communication and Tactical Networking (final report in process)

CHAPTER FIVE

Anticipating Intelligent Systems and Autonomy

5. ANTICIPATING INTELLIGENT SYSTEMS AND AUTONOMY

NUMBERS AND DISAGGREGATION ▪ RANGE ▪ DANGER ON AND ABOVE SEA SURFACE DRIVE WARFARE UNDERSEA

The U.S. is generally believed to have the best military technology in the world. Coupled with outstanding professional soldiers, sailors, airmen, and marines, military technology contributed to the U.S.' role as the leading global power. However, the cost of technology and its associated equipment remains high, which has had cascading effects.

DoD resources are stretched thin because of increasing global demands on the military and the constraints of limited budgets. In this situation, the generally high cost of new technology has significantly limited the quantities that can be acquired. In turn, the few systems that are fielded often serve as prime targets for adversaries. These factors together tend to reduce U.S. willingness to engage due to the cost, in dollars and lives, of losing these assets.

A promising approach to address this challenge is to use lower cost, unmanned systems more extensively, to complement existing systems and to provide alternatives to these systems going forward. While lower cost systems will often be less capable and support a more limited mission scope, they can be acquired in larger numbers and, as illustrated in *Technology and Innovation Enablers for Superiority in 2030 (2012 summer study),* quantity can be an important quality factor. Furthermore, low-cost systems in large numbers can be cost-imposing, especially when it costs more for adversaries to defeat them than for the U.S. to acquire them.

Building trust in autonomous systems is challenging yet achievable

With recent advances in artificial intelligence, autonomy is being rapidly adopted for a diverse and expanding set of commercial applications, such as self-driving cars, factory automation and manufacturing, fraud detection, and medical diagnostics.

> **Every application of autonomy engages both human and machine throughout the system lifecycle.**

When the DoD considers the use of autonomy its applications, the Department raises the key issue of trust, particularly for lethal systems. Significant public discussion has raised concerns associated with lethal autonomous weapon systems. These discussions are sometimes cast in the context of "killer robots" and accompanying ethical and emotional issues.

While technical issues will indeed require development to improve trust in autonomous systems, the first step in dealing with the public concerns about lethal autonomous weapons systems is to recognize that a truly fully autonomous system does not exist. Furthermore, the DoD Directive 3000.09 (2012) includes a very clear and explicit policy requiring "appropriate levels of human judgment over the use of force."

DoD is increasingly employing autonomous capabilities across a diverse array of systems. Every application of autonomy engages both human and machine throughout the system lifecycle. Certain roles will remain the purview of the human, others will be shared, and some tasks will be implemented solely by machines. While the specific roles of humans will vary by mission and over time, all autonomous systems are supervised at some level within the bounds set by the system designer.

The DoD can take several steps to enhance confidence in autonomous systems, as explored in the DSB *Summer Study on Autonomy (2015)*. For example, a key design task is to ensure intuitive and effective human-system interfaces that facilitate operator understanding of the computer's state of knowledge and the basis for decisions that will be made by the computer. Developing effective interfaces can be assisted by the use of model-based design techniques that employ system simulations that grow in fidelity as the design matures and that enable operators to interact with the autonomous system through all phases of its development. This simulation-based approach provides valuable design feedback that enhances the operators' understanding of the computer's functions and ultimately enables the human and autonomous system to interact and engage as a team.

A system simulation can evolve throughout the design process and, when mature, serve as an effective tool for the test and evaluation required to accept and certify an autonomous system, particularly a complex intelligent system based on non-deterministic software that does not lend itself to exhaustive regression testing.

FRAMEWORK FOR THE DESIGN AND EVALUATION OF AUTONOMOUS SYSTEMS

Cognitive Echelon View
As component agent and roles increase in autonomy, critical issues shift to relationships and coordination across roles and echelons

- Mission
- Section
- Vehicle

Scope of control

Mission Dynamics View
Where cognitive functions can assist

- Initiation
  Plan, including delegation and bounds
- Implementation
  Action failures, obsolete portions of plans
  Mission Complete
- Termination

Complex System Trades Space View
Whether explicitly made or not, system level performance trades result from design

- Responsibility: Short- vs. long-term goals
- Perspectives: Local vs. global views
- Impact: Centralized vs. distributed
- Plans: Efficiency vs. thoroughness
- Fitness: Optimality vs. resilience

  Performance / Variation from nominal conditions

An autonomous system reference framework highlights the allocation of cognitive functions between the human operator and the computer. *The Role of Autonomy in the DoD Systems (2012).*

Using the simulation environment to augment operational testing, testers can explore the full operating envelope, including complex boundary-condition cases, to validate the system's performance relative to its specifications.

Perhaps somewhat paradoxically, many current unmanned systems require significant numbers of human operators. In fact, the Air Force has commented that "manning their unmanned systems" is its most challenging manning problem. The DSB identified the failure to allocate cognitive functions explicitly between the operator and the computer as a primary cause of the manning problem. *The Role of Autonomy in DoD Systems (2012)* recognized that this allocation was likely to be dynamic, varying over the course of a mission as conditions changed and complexity increased. It proposed a framework for use during both the requirements and design process to focus attention on this critical development task.
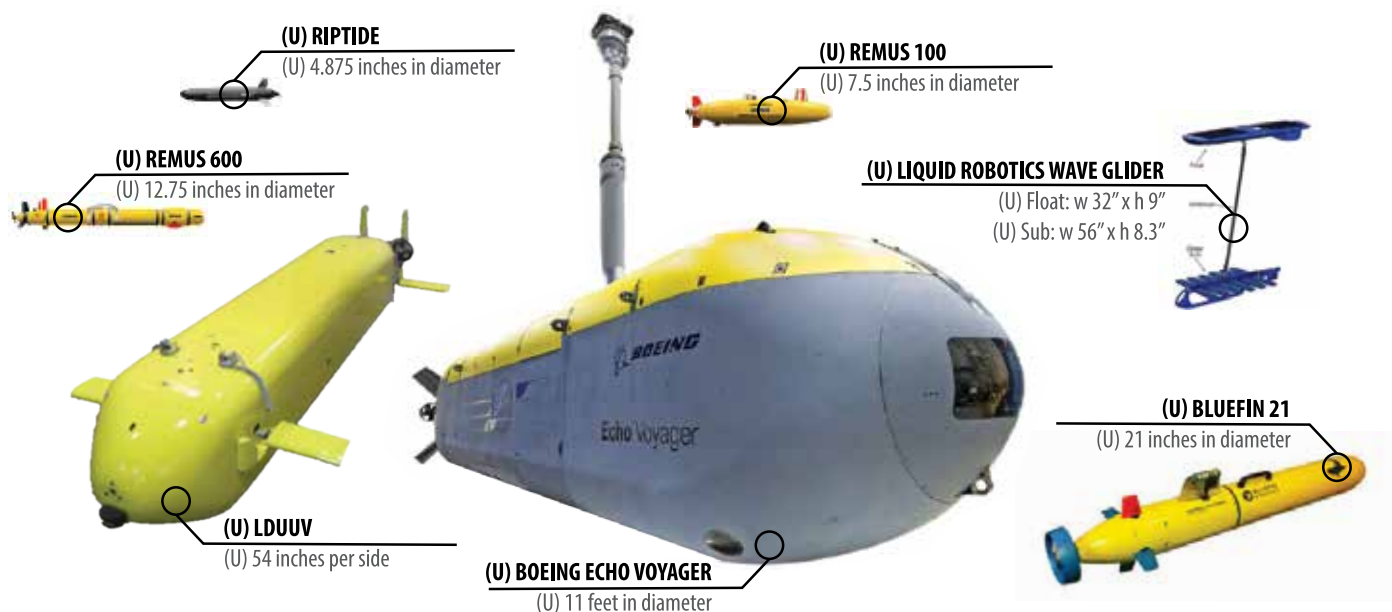
Finally, to grow capability over time in a cost-effective manner as the technology evolves, it remains important to separate the software from the hardware platform and to ensure the use of an open architecture with government ownership rights. This approach better enables the adoption of new technology, facilitates multi-platform application of the software, and avoids vendor lock.

Development of low-cost platforms requires a new acquisition mindset

The traditional DoD requirements-driven development process collects a set of capabilities desired by the operational community into a requirements document for a new system. Because the acquisition process is lengthy and the number of new programs is limited, the "system" is motivated to include as many desirable capabilities as possible in the requirements. In turn, cost is generally considered as one of a set of characteristics that compete with each other in a systems engineering trade study. As military capability with little direct responsibility for development budgets and affordability stands as the primary motivation for the operational community, the trade studies often result in a complex and expensive design of systems that can then only be acquired in limited numbers.

To develop low-cost systems that can be acquired in large numbers to complement very capable front-line equipment, the DoD should treat cost differently. A target cost per unit should be established upfront as a non-tradeable

(U) RIPTIDE
(U) 4.875 inches in diameter

(U) REMUS 100
(U) 7.5 inches in diameter

(U) REMUS 600
(U) 12.75 inches in diameter

(U) LIQUID ROBOTICS WAVE GLIDER
(U) Float: w 32" x h 9"
(U) Sub: w 56" x h 8.3"

(U) BLUEFIN 21
(U) 21 inches in diameter

(U) LDUUV
(U) 54 inches per side

(U) BOEING ECHO VOYAGER
(U) 11 feet in diameter

Several commercial unmanned undersea vehicles have been adapted for military use at a far lower cost than a traditional D0D acquisition program, as described in *Next Generation Unmanned Undersea Systems (final report in progress)*.

requirement, and capabilities should be selected that provide the most relevant military capability within the target cost even if this capability is less than potentially achievable or is limited to only a subset of potential missions.

By approaching the design process from this new perspective, the DoD can eliminate or reduce some traditional requirements because of the resulting low cost and ability to acquire and deploy large numbers. For example, one of the most costly requirements is platform survivability, crucial for expensive manned platforms and drives the development of advanced technologies for aircraft signature reduction (stealth), armored vehicle protection (advanced materials and adaptive armor), and indefinite submersion and quieting of submarines (nuclear power and long-life batteries). With unmanned systems, human lives are not at risk, so if costs remain low enough, the DoD can consider the vehicle attritable and may not require costly survivability technologies. Depending on the mission, the Department can also avoid costs for recovery with an expendable system, as has been the case for missiles, munitions, and other systems. In many of these situations, it may cost the adversary more to detect, track, and defeat a low-cost platform than it costs

the U.S. to acquire and deploy it. This sets up a favorable cost-exchange ratio that does not often exist with more complex equipment.

The DoD can also control costs by reusing or adapting existing military or commercial platforms for new missions by focusing on payloads and mission capability rather than on potentially exquisite new platforms. In particular, an increasing number of opportunities to leverage commercial platforms has accompanied the explosion of commercial activity related to unmanned air and undersea vehicles. For example, the DSB report *Next Generation Unmanned Undersea Systems (final report in process)* identified an array of commercial unmanned undersea vehicles developed for multiple purposes (e.g., oceanography and oil and gas exploration). The Navy may adapt each of these platforms for its missions at a cost and development time significantly lower than those anticipated, such as for the custom-built Large Diameter Unmanned Undersea Vehicle (LDUUV), as initially conceived. The report also suggested designs for several reference missions to demonstrate the potential for low cost missions and mission payloads. These leverage commercial platforms with costs on the order of $1 million; mission payloads are expected to be in the same cost

range as the platforms. The report also explored using very large unmanned undersea vehicles as a means for cascaded delivery of smaller systems, which could enable manned submarines to take on more complex and challenging tasks. Several commercial unmanned undersea vehicles have been adapted for military use at relatively low cost.

Experimentation and learning are required to validate proposed concepts

In a series of studies, the DSB has exploited the principle of low-cost systems in large numbers to suggest approaches to a wide range of challenging defense problems, including time-critical strike from strategic standoff (*Time Critical Conventional Strike from Strategic Standoff, 2009*), air dominance in an anti-access/area-denial environment (*Air Dominance, final report in process*), cruise and ballistic missile defense (*Defense Against Advanced Ballistic and Cruise Missile Threats, final report in process*), complementing manned submarines with unmanned systems to extend U.S. undersea advantage (*Next-Generation Unmanned Undersea Systems, final report in process*), and expanding the capabilities of indirect fires for the Army (*Integrated Fire Support in the Battlespace, 2004*). In some of these cases, the proposed point solution was not low-cost in an absolute sense because the long range needed to address the required capability cannot be achieved inexpensively. Even in these situations, however, the solution was less expensive and relied on greater numbers than the manned alternatives.

Often, the proposed low-cost platforms or rounds are intended to work in concert with high-end manned systems and expand capability by enabling new concepts of operations, including decoys, deception, and dispersion. In addition, overall survivability is improved by increasing both the number of and the area with potential targets that an adversary needs to address, which can provide the U.S. with an asymmetric advantage that complicates and increases the adversary's cost of defense. Lethality can also increase in configurations such as the Navy's concept for distributed lethality, which, in a

sense, disaggregates offensive capabilities by putting more weapons on more platforms. This increase in number of targets raises the adversary's engagement cost to levels that are unaffordable for them and, consequently, the need for the U.S. to defend each platform can decrease resulting in lower system costs.

While innovative point designs may exist for challenging problems, designs and their associated concepts of operations should be validated through a robust experimentation program that involves and solicits feedback from operational personnel. These experiments should be constructed as learning exercises in which it is possible and even acceptable to fail rather than just demonstrate performance. The DSB expects that both system requirements and concepts of operation will change based on experimentation results. However, the DoD should structure the programs so that operational forces may use residual assets that demonstrate utility.

To control cost and accelerate acquisition, the initial deployed system should be the simplest, most mature configuration that holds meaningful military value, rather than maximum potential value. The system architecture design should support iterative development and growth in capability to enable new missions as technology becomes available.

New infrastructure is required to support low-cost systems

In addition to low-cost platforms, defense infrastructure is of particular importance to effective mission capability. The DSB identified three infrastructure areas as especially significant:

- Intelligence, surveillance, reconnaissance, and targeting

- Command, control, and communications

- Guidance, navigation, and control

Information from both national technical means and tactical sensors remains crucial to identifying and locating potential targets accurately. One of the key challenges is ensuring alignment of

In many situations the significant time it took to complete the decision process meant that the added value of extreme weapon speed did not justify the additional cost. None of the scenarios exposed a need for "one hour, global range delivery."

the coordinate systems of the sensors and the tactical platforms so that target coordinates can be transferred without error. This process has become easier in recent years because of effective gridlocking and the ubiquitous availability and use of the Global Positioning System, although there still can be problems on the tactical battlefield. One of the key advantages of arming Predator unmanned aircraft with Hellfire missiles in the recent conflicts is that it co-located a sensor with the weapon, effectively eliminating previous gridlock issues.

As battlespace complexity increases with large numbers of low-cost platforms, C3 systems that provide coordination and control among the various systems take on greater importance. A C3 system is more than just computers and communications gear. The decision-making process, an inherently human endeavor, often stands as the long pole in the decision timeline, particularly when rules of engagement require minimizing collateral damage. In many situations the significant time it took to complete the decision process meant that the added value of extreme weapon speed did not justify the additional cost. None of the scenarios exposed a need for "one

hour, global range delivery." There appears to be nothing unique or compelling about one hour.

The DoD needs intuitive human-system interfaces to enable effective human supervision of autonomous systems. It remains critical for all missions to ensure that the operator understands and trusts the autonomy, especially those with lethal consequences where DoD policy requires the employment of appropriate human judgment. Simulations running in both the onboard system and in a control center with frequent comparison of results and situational awareness can be a useful mechanism for building trust, particularly with short decision times or limited communications bandwidth.

Low-cost platforms depend on reliable, accurate, and cost-effective positioning. In nearly all scenarios, GPS combined with a relatively low-cost inertial navigation system provides sufficient accuracy to meet mission requirements. A difficulty arises when GPS is either jammed or unavailable for some other reason, such as being indoors or underground. The low power of the GPS signal created significant and justifiable concerns about jamming, and extensive research exists on

alternatives to GPS. While the DoD has made progress, no single silver-bullet alternative exists that provides comparable accuracy. Solutions to GPS denial will likely rely on integrating inputs from a number of different sensors and data sources. One of the design challenges for these GPS-denied situations will be to trade the cost of a potentially complex multi-sensor integration solution providing increased accuracy against the cost for the increased number of lower accuracy systems required to satisfy the mission.

U.S. must prepare for adversary use of low-cost unmanned systems

The U.S. is not alone in considering how to exploit low-cost unmanned systems; highly capable technology is available both globally and commercially. In particular, commercial unmanned aircraft are readily available in the global marketplace at low cost, and unmanned undersea vehicles can be purchased for modest cost. In addition, nearly all research universities with engineering programs offer autonomous robotics projects as standard curriculums. Thus, there exist few barriers to entry, as both the systems and the knowledge to use them have become broadly available. Consequently, U.S. adversaries will inevitably use these technologies against the nation.

The U.S. must prepare to face these systems and develop approaches to defeat them. This will require that wargames, experimentation, and operational exercises include low-cost unmanned systems in the opposing force arsenal. In these exercises, the Department must take care to avoid only mirroring the way the DoD plans to use the capability. Adversaries will likely hold more permissive rules of engagement than the U.S., which requires that the DoD opens the aperture on usage to create the full range of threats that will almost certainly be encountered.

Supporting DSB reports

Integrated Fire Support in the Battlespace (2004)

Time Critical Conventional Strike from Strategic Standoff (2009)

The Role of Autonomy in DoD Systems (2012)

Technology and Innovation Enablers for Superiority in 2030 (2012 summer study)

Autonomy (2015 summer study)

Air Dominance (final report in process)

Next-Generation Unmanned Undersea Systems (final report in process)

Defense Strategies for Advanced Ballistic and Cruise Missile Threats (final report in process)

CHAPTER SIX

Supporting Stabilization, Reconstruction, Peacekeeping, and Nation Building

6. SUPPORTING STABILIZATION, RECONSTRUCTION, PEACEKEEPING, AND NATION BUILDING

WINNING THE PEACE

The DSB vision for enhancing U.S. effectiveness in the transition to and from hostilities includes two dimensions:

- **Management and planning discipline.** The management discipline used by the Military Services to plan and prepare for combat operations must extend to peacetime activities, and to stabilization and reconstruction operations, in the DoD and across the whole of government.

- **Building and maintaining certain fundamental principles and capabilities now lacking critical to success in stabilization and reconstruction.** These capabilities include establishing clear objectives and ensuring comprehensive planning and oversight; improving strategic communication; developing local cultural understanding and intelligence; effectively integrating contractor support throughout planning and operations; and most importantly, improving relevant personnel development.

The DoD must plan for stabilization and reconstruction operations

Stabilization and reconstruction operations typically last five to eight years—significantly longer than typical combat operations. Further, since the end of the Cold War, the United States began stabilization and reconstruction operations every 18 to 24 months. That frequency coupled with the length of these operations indicates the significant requirement for skilled personnel in support of these operations. While technological advances can contribute to U.S. capabilities, they are not likely to materially reduce the time needed for stabilization and reconstruction or the requirement for in-country forces.

Even with predicted political reluctance, the U.S. military expeditions to Afghanistan and Iraq will unlikely be the last such excursions.

While technological advances can contribute to U.S. capabilities, they are not likely to materially reduce the time needed for stabilization and reconstruction or the requirement for in-country forces.

While U.S. armed forces remain extremely capable of projecting force and achieving conventional military victories, success in achieving U.S. political goals also requires success in maintaining political stability during stabilization and reconstruction operations that follow hostilities. Further, orchestration of the instruments of U.S. power in peacetime might obviate the need for many military excursions; or, failing that, at least better prepare the U.S. to achieve political objectives after hostilities during stabilization and reconstruction operations.

Taking lessons from history, the DSB observed the importance of comprehensive planning and preparation before, during, and after conflict in order to secure both short-term and longer-term stability once hostilities cease. Issues the DSB addressed include: identification of the information and intelligence required to successfully conduct stabilization and reconstruction operations; best use of the National Guard and Reserves with their civilian sector skills; language and cultural training; and campaign planning and exercising for stabilization and reconstruction missions on par with what the U.S. does for combat missions.

In partnership with the Department of State, the National Security Council (NSC), and other elements of the Executive Branch, the Department of Defense has made modest progress toward planning for the next stabilization mission, although much more remains to do.

The DoD needs investments to adequately prepare for stabilization

Objective planning and oversight. Success depends on a stronger partnership and closer working relationships between the DoD and the Department of State toward making stabilization and reconstruction missions one of their core competencies. Moreover, both departments need to augment their existing capabilities for stabilization and reconstruction. The DoD has not yet embraced stabilization and reconstruction operations as an explicit mission with the same seriousness as combat operations.

The Department needs new coordination and integration mechanisms to bring management discipline to the continuum of peacetime, combat, and stabilization and reconstruction
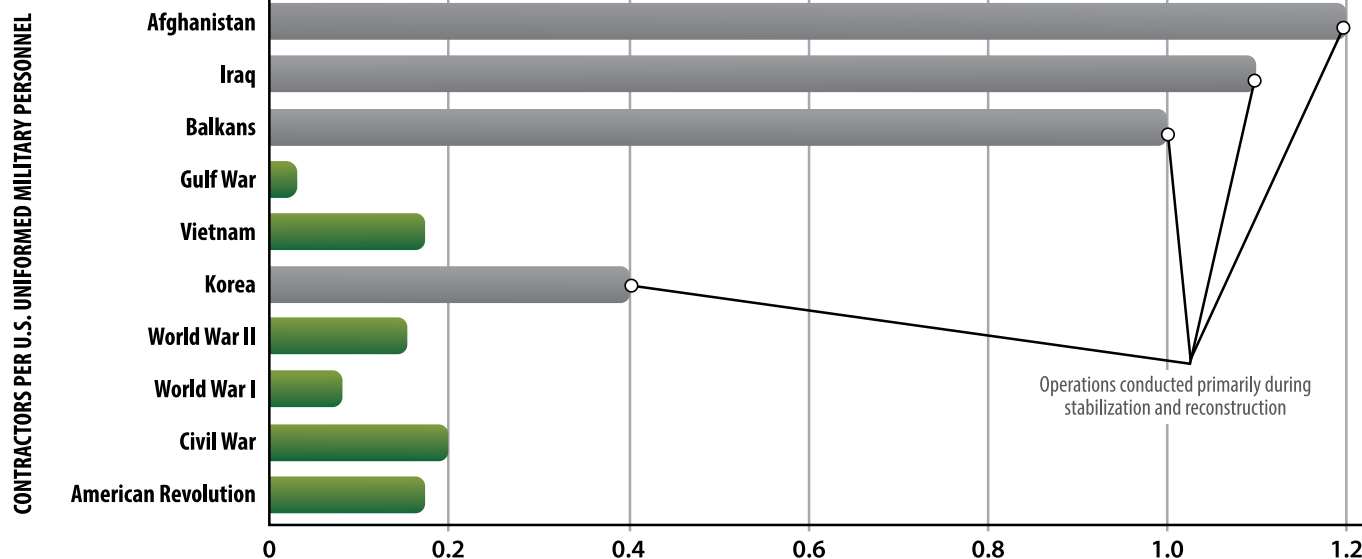
Contract support of deployed military operations has been used since the American Revolution.
(DSB Report on *Contractor Logistics in Support of Contingency Operations, 2014*)

operations. For countries with high risk of U.S. intervention, the President or NSC would direct the initiation of a robust planning process. The elements of that process should include:

- During high likelihood of U.S. intervention, full-time planning activities may continue for months or years and must be staffed by individuals, from all involved agencies, who maintain genuine, deep expertise in the culture of the countries of interest and in needed functional areas. The DoD must create Joint interagency task forces composed of senior government executives and military officers who operate in the particular country or area of interest to ensure coordination and integration of the activities of all U.S. personnel "in-country."

- When intervention begins, the Department should establish a center with country and functional expertise should support the contingency planning and integration task forces and the joint interagency task forces. The center coordinates augmentation of skills and expertise of the government task forces, supports the planning process, and provides the necessary continuity.

- The DoD must identify a focal point at each regional Combatant Command. The most likely candidate is the combined/joint forces land component commander.

Strategic communication. Encompassing public affairs, public diplomacy, international broadcasting, information operations, and special activities, strategic communication remains vital to America's national security and foreign policy. The strategic communication environment and requirements changed considerably because of many influences, including a rise in anti-American attitudes around the world; the use of terrorism as a framework for national security issues; the widespread use of social media as a communication vehicle; and the volatility of Islamic internal and external struggles over values, identity, and change. U.S. adversaries are using strategic communication very effectively against the U.S. The country needs an integrated coherent strategic communication capability and operation to support each of its national objectives.

Knowledge, understanding, and intelligence for the 21st century. The knowledge required to be effective in conducting stabilization and reconstruction operations differs from the military

knowledge required to prevail during hostilities, but no less important. Knowledge of a nation's security interests and external relations; armed forces; the local political scene; internal social, cultural, and economic conditions; security; and social and economic well-being remain as important to stability operations as the knowledge of the enemy order of battle during hostilities. Often U.S. forces relied too heavily on remote sensors versus on the ground intelligence and understanding of the cultural nuances of the adversary *and* the local allies. The DoD needs to treat understanding of culture and developing language skills as seriously as it treats learning combat skills: the Department needs both for success in achieving U.S. political and military objectives.

Effective stabilization and reconstruction, and intelligence for these activities, must reflect a whole-of-government effort and whole-of-government capabilities. The U.S. requires the means to transition into and out of hostilities, and nowhere is this need more salient than for counterinsurgency missions (*Transition to and from Hostilities (2004 summer study)*. Addressing the entire life-cycle requires knowledge management capabilities that serve a wide variety of U.S. Government departments and agencies—DoD, Department of State, the intelligence community, and so on. A national intelligence mission for counterinsurgency would facilitate efficient and effective intelligence support enabling a knowledge management capability supporting whole-of-government efforts and which would encourage use of a broader range of information sources that go beyond legacy intelligence collection.

The U.S. government does not invest adequately in the development of social and behavioral science information critically important for counterinsurgency and national security in general. Many, if not most, specific requirements for intelligence, surveillance, and reconnaissance center on population and are not exclusively solvable with hardware or hard, physical science solutions. One senior intelligence officer with years of field experience pointed out that 80 percent of useful operational data for counterinsurgency does

not come from legacy intelligence disciplines. Good intelligence exists outside the traditional intelligence organizations. The U.S. needs anthropological, socio-cultural, historical, human geographical, educational, public health, and many other types of social and behavioral science data and information to develop a deep understanding of populations (*Understanding Human Dynamics, 2009*). Such data, collected and analyzed using the scientific method, remain vital to counterinsurgency success.

Private sector support to stabilization and reconstruction activities. The Department must establish organizations and approaches to exploit its "fifth force provider"—the private sector. The report established that contractor support holds as an essential element of employing the private sector. The Department has used contractors in the support of our troops since the Revolutionary War. For the majority of the time in Iraq and Afghanistan, more than 50 percent of the U.S. supported forces in the field were contractors. The report concluded that well-managed contracted support is, and will continue to be, a necessary tool for future contingency operations. Realizing all the benefits from contracted support of deployed military forces hinges on acceptance and integration of such support in planning and exercises as a key component of the total force. This culture change in the Department of Defense just began, but will need vastly improved leadership and organization at all levels before full implementation, before the next unpredictable event that will mobilize the U.S. military.

The government instruction for preparing various status of forces agreements must include non-government entities. Such agreements must preclude controversy and consequence surrounding tax law and subject of individuals to local criminal law. Ignoring such provisions will limit private sector participation.

Personnel development. The development of effective personnel who can be effective in this non-combat mission represents the most important element of a complete strategy for preparing for stabilization and reconstruction operations.

- Leadership development. The nature of stabilization and reconstruction operations places enormous burdens on junior officers and non-commissioned officers and the units that they command. Presently, they must make decisions that traditionally believed to be far above their pay grade. For this mission, small unit performance represents the key to success. The potential key message from this report is that small units and their leaders are strategic assets and the department should resource them accordingly. Proper training and leader development can make a significant impact sooner than many other investments in doctrine, organization, training, materiel, leadership, personnel, or facilities. Training has been a significant asymmetric advantage to U.S. forces over the course of the last two decades.

- Professional military education. The challenges of the 21st century demand that senior officers be thoroughly educated and culturally attuned while in command positions. The DoD needs to reform its personnel system so that fast track officers hold the opportunity to attend the most prestigious graduate schools to obtain advanced degrees in subjects such as area studies, languages, cultural studies, and military history.

- Use of Reserve Forces. The Reserve and National Guard forces remain a very important asset that must be cultivated and prepared to support these operations. They often bring more varied experience than the regular force and stand ready to act once they hit the ground. However, they too need to understand the local cultures that they are likely to face and this requires training.

The DoD needs broad organizational changes

The DSB examined a number of organizational approaches to the establishment of an entity to prepare for future stability operations. Such an organization would be useful in pre- and post-hostility operations. It would focus on supporting national objectives in each selected region. It would manage the pre-hostility (Phase 0) and post-hostility counterinsurgency activities with a focus on influence and non-traditional powers like strategic communication and reconstruction to support the DoD's national objectives versus military force. In the end, the DSB decided that such a recommendation on organization is so all-encompassing that it transcends adding an assignment to an existing organization. The Board sees this recommendation as much more than a new focus; it contains strong parallels to founding a new mission-oriented agency. The major topic of open discussion in the DSB task forces on pre- and post-hostilities is in regard to the appointment of an executive agent to focus on the implementation of said recommendations. Instead, the DSB recommended that the Secretary of Defense, along with the head of the intelligence community, jointly compose a course of action. The DSB believes that this action will involve beginning a new organization, and whether that organization reports to the Secretary of Defense, the Joint Chiefs of Staff, the head of intelligence or a military service is a matter for them to decide.

The DSB strongly urges Combatant Commanders to broaden the aperture of their disciplined planning process to encompass not only combat, as now, but also the peacetime employment of military instruments and the Department's capabilities for stabilization and emergency reconstruction. This role also includes humanitarian support currently in the scope of the Combatant Commands.

For that expanded planning activity to have meaning, defense intelligence organizations should maintain and execute a portfolio of concomitant intelligence campaign plans supporting the aforementioned regional combatant commanders' operations plans.

Executing the stabilization and reconstruction operational elements of campaign plans will require vastly expanded and improved stabilization and emergency reconstitution capabilities, and the DSB asks the Military Services to ensure those capabilities are available to the regional combatant commanders. In planning for the

provision of those capabilities, the Military Services need to perform quantitative analysis of their likely expected needs with at least the same veracity as they do for combat force structure. The Military Services should also take skills in languages and culture as seriously as they take skills in combat; otherwise the nation may win the war but will surely "lose the peace."

In addition to strengthening capabilities within the DoD, the DSB urges the Secretary to use his considerable influence to propel needed changes that span other government's agencies and departments or which center on cabinet departments other than Defense.

The Secretary should lend his support to the efforts of other departments and agencies as they undergo transformation, particularly in their approach to instituting management discipline for contingency planning and for maintaining contingency capabilities. Finally, the Secretary should urge the establishment of an effective national strategic communication capability and lend the DoD's resources and capabilities to this effort, as appropriate.

DoD must be prepared to win the peace

If the DoD implements the DSB's recommendations, what will the U.S.' adversaries face?

An adversary will face the focus of the full range of the U.S. Government powers in peacetime from security assistance to special operations to head off stability operations or major combat operations. If the DoD cannot avoid stability operations, an adversary will face a comprehensive pan-government activity backed by an operational plan and pan-intelligence community supporting intelligence plans.

In order to achieve these outcomes, the U.S. must prepare to anticipate the long-lead capabilities needed for the future stability and influence operations. The government must clearly assign roles, responsibilities, accountability, and

resources to departments and agencies. It must focus on issues before crises occur and maintain contingency capabilities: planning, exercising, and deep expertise in regions of interest. It must prepare to invest in the human resources to win the peace: linguists, analysts, and case officers.

In order to achieve these capabilities, the DoD must prepare to provide adequate resources. The alternative is more expensive in both dollars and lives. While the DSB did not undertake a rigorous effort to derive the costs of implementing these recommendations, nor did it attempt to enter the "trade space" in which investment in these capabilities would be offset by savings associated with cuts to current capabilities, cost savings appear almost certain. Approaches that rely on population-centric intelligence would significantly reduce the likelihood of costly, major combat operations. Building a national infrastructure of country- and region-specific experts, reinvigorating the Foreign Area Officer program, and establishing relevant intelligence programs within the major intelligence agencies would represent a fraction of the cost of a major military intervention, and could save millions of human lives lost in more traditional hostilities.

Supporting DSB reports

Transition to and from Hostilities (2004 summer study)

Institutionalizing Stability Operations within DoD (2005)

Force Protection in Urban and Unconventional Environments (2006)

Understanding Human Dynamics (2009)

Counterinsurgency Intelligence, Surveillance, and Reconnaissance Operations (2011)

Contractor Logistics in Support of Contingency Operations (2014)

CHAPTER SEVEN

Preparing for Surprise

7. PREPARING FOR SURPRISE

One of the clear messages of the last ten to 15 years is that too often world events will not unfold as desired or even predicted and that the U.S. must be prepared to deal with the unanticipated. The DoD must improve the cultural understanding of the nature of surprise, how to reduce its occurrence, how to prepare for it before it occurs, and how better to deal with it when, inevitably, it does occur. Reinvigorating flexibility and innovation in strategies, tactics, forces, acquisition system, and in the industrial base rapidly becomes a requirement rather than a "nice-to-have."

Military forces must be able to adapt

How they train and exercise
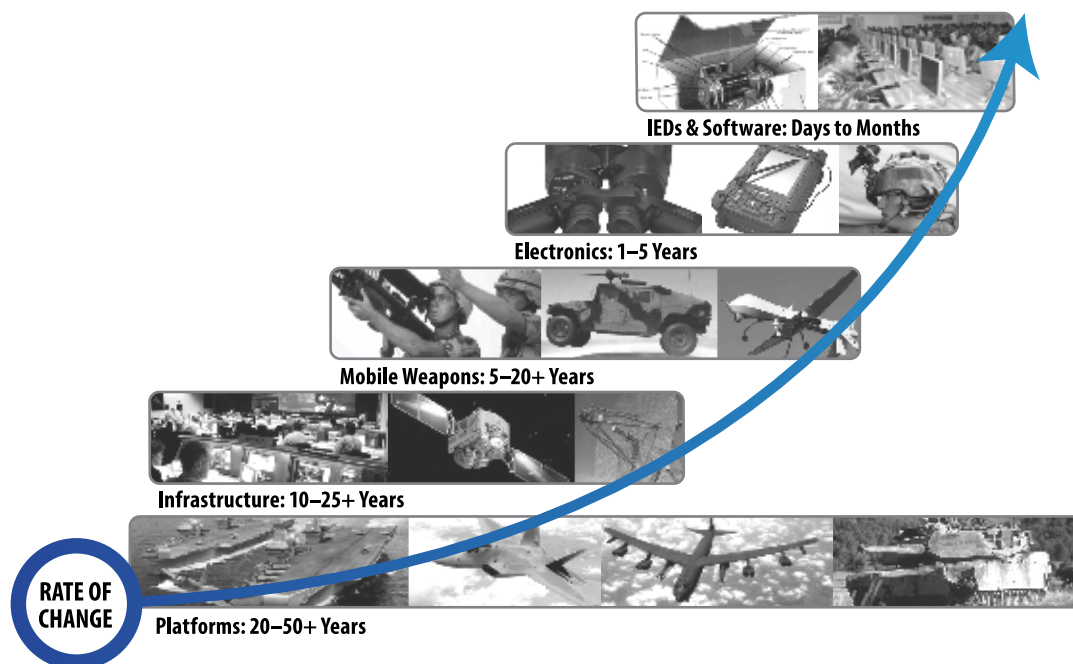*How they incorporate learning*
How they operate in the field

Given the inevitability of surprise, one of the principal keys to dealing with it will be the ability to adapt, sometimes to unforeseen operational tactics by an adversary, sometimes to unforeseen weapon systems or characteristics, and sometimes to a combination of both. The DoD's ability to adapt, rapidly and effectively, will depend upon the flexibility it builds into two interrelated but distinctly different domains: how the Department develops and trains the troops and how it specifies and builds the systems on which they depend.

To prevail in a tactical environment of uncertainty and surprise, operational flexibility and the ability to adapt rapidly to unexpected circumstances are clearly necessary attributes. To achieve this, the Department needs to instill a "culture" of adaptability in its forces, from the lowest level soldier to senior officers.

Red teaming

Red teaming is one of the most sorely needed activities to improve adaptability. In its simplest form red teaming entails structured challenging of decisions, accepted ways of doing things, system constructs and architectures, tactics and operations, and anything else that may be subject to something beyond the control of the user, developer, or creator. Issues such as enemy tactics,

IEDs & Software: Days to Months

Electronics: 1–5 Years

Mobile Weapons: 5–20+ Years

Infrastructure: 10–25+ Years

RATE OF CHANGE

Platforms: 20–50+ Years

The rate of change in defense systems was examined in the DSB Report on *Enhancing Adaptability of U.S. Military Forces, 2011.* As the DoD has adopted more unmanned, mobile, and software-dependent systems, adaptability has become a critical performance parameter.

operational environments, threat characteristics, and adversary responses to the DoD's actions or system improvements all are things that are beyond the Department's control and can affect success or failure on the battlefield. The talent, expertise, creativity, and independence of the red teamers represent critical characteristics of successful red teaming. Senior leadership holds equally important role in creating an environment that recognizes and fully embraces the importance and value of aggressive red teaming with a primary role to challenge accepted views and the status quo. This must be conveyed throughout the organization, be it operational or materiel development. At whatever level the Department conducts red teaming, leadership must also provide "top cover" for the red team, to prevent the results from dismissal or marginalization. When implemented successfully, red teaming can be invaluable in getting ahead of whatever an adversary might do and preparing forces for dealing with unanticipated circumstances.

Training and exercising in stressing environments

Current military exercises are often more demonstrations than good learning opportunities.

The DSB recognizes the need for some degree of show and tell, particularly in large-scale exercises, but troops also need to be subject to tactics, environments, and weapon characteristics for which they are not totally prepared. Clearly, the troops are better off with the opportunity to learn how to adapt and fight through issues on the training field rather than scrambling when lives are at stake.

Numerous examples exist of the DoD stopping exercises as operations start to fail, rather than letting them continue so that lessons can be learned, troops have the opportunity to adapt, and most importantly, a culture of always having to deal with the unexpected is created. In particular, the Department needs training and some degree of exercising in severely challenged sensor, communications, and geospatial environments of electronic warfare, cyber intrusion, loss of space capabilities, etc. It should not surprise the DoD when today's adversaries attempt to create these challenging environments and the Department needs to be prepared to successfully negate and/or operate in them.

The learning associated with both robust red teaming and training and exercising should

Perhaps even more important, is discovering and seizing on opportunities to create uncertainty and inflict surprise on the opponent. Such opportunities may more likely present themselves when looking at a situation with fresh eyes or viewpoint, rather than in more tried and true conventional ways.

encourage operational units and their commanders to embrace alternative viewpoints at all levels. Willingness and indeed eagerness to examine a wide range of possible options on how to deal with the unexpected can yield a two-sided advantage. On the one hand, it may provide a response to something an adversary has done that is well outside the realm of previously considered or conventional responses and which can offer unusual leverage. But equally, or perhaps even more important, is discovering and seizing on opportunities to create uncertainty and inflict surprise on the opponent. Such opportunities may more likely present themselves when looking at a situation with fresh eyes or viewpoint, rather than in more tried and true conventional ways.

Encouraging alternative viewpoints

All of this argues for achieving a balance between the necessity for non-chaotic, organized behavior of troops on the battlefield; and non-predictability, flexibility, and adaptability in responding to the unexpected, and in turn imposing the unexpected on the adversary. A U.S. edge in training and a culture of willingness to embrace aggressive self-examination and diverse viewpoints can enable both to occur as needed.

Operational adaptability should be an inherent strength of our forces and operational surprise should be nurtured to work in our favor.

Military systems must be able to adapt

How they are specified

How they are architected

How they are upgraded

How they adapt in the field

Ensuring the Department provides its forces with intrinsically adaptive systems appears as important as developing adaptive forces. The knowledge that DoD will face surprise largely drives the motivation for maintaining adaptive systems, and it must assume the systems built will require operation in ways and in conditions the Department will never completely be able to predict. This reality, combined with the ever-increasing need for speed and learning, drives the DoD's need for adaptive systems. U.S. forces and capabilities will need to anticipate change to the extent possible, sense and adjust to the change as quickly as feasible; this also remains true for the DoD's acquisition processes and the systems produced. The Cold War

legacy of many of today's fielded major acquisition weapon systems and the acquisition process that built them emerged from a much more clearly defined threat and set of potential scenarios. Today, the DoD needs different requirements methods, acquisition approaches, and design principles to deal with the variety of futures the U.S. faces and the inevitability of surprise.

Characteristics of adaptable systems

Speed remains key to adaptive systems; they must be designed to intrinsically be able to keep pace with the increasing rapid advance in technology, change as the adversary learns and adjusts, and as the DoD's adaptive war fighters learn new ways to use the equipment. Adaptive systems must be honed by realistic exercising and red teaming and able to be resilient to execute their mission despite degraded conditions. These operations may encounter natural degraded environments such as weather or induced degradation such as cyber, electronic warfare, or space attacks. Most successful historical cases of delivery of adaptive systems had a strong alignment between the development team, testers, program management, and the operational user. In many cases the

timeline of delivery was driven by an operational timeline versus an "enterprise" timeline.

As might be expected from this problem statement, there is not a universal approach for designing adaptive systems. Instead, basic principles of design should guide the design. For example, a system that can used for multiple roles and missions is adaptive by definition—the oft-cited B-52 as a positive example—it is used today in ways much different than envisioned for its original cold war strategic deterrence mission. Conversely, it is also true that multi-mission approaches are not always the most adaptable solution—the Joint Tactical Radio System as the oft-cited negative example—in hindsight the design approach of combining the full waveform set in a single software defined radio was overly complex, expensive, and fundamentally flawed. In these cases, the key step is performing upfront a realistic business case for alternative approaches, and looking skeptically at technology maturity and complexity of the design and resultant risks in engineering development before deciding which path to choose. The challenge is to do this in a way that does not inhibit new concepts, new technologies, or the application of innovation. This upfront work informs whether to pursue
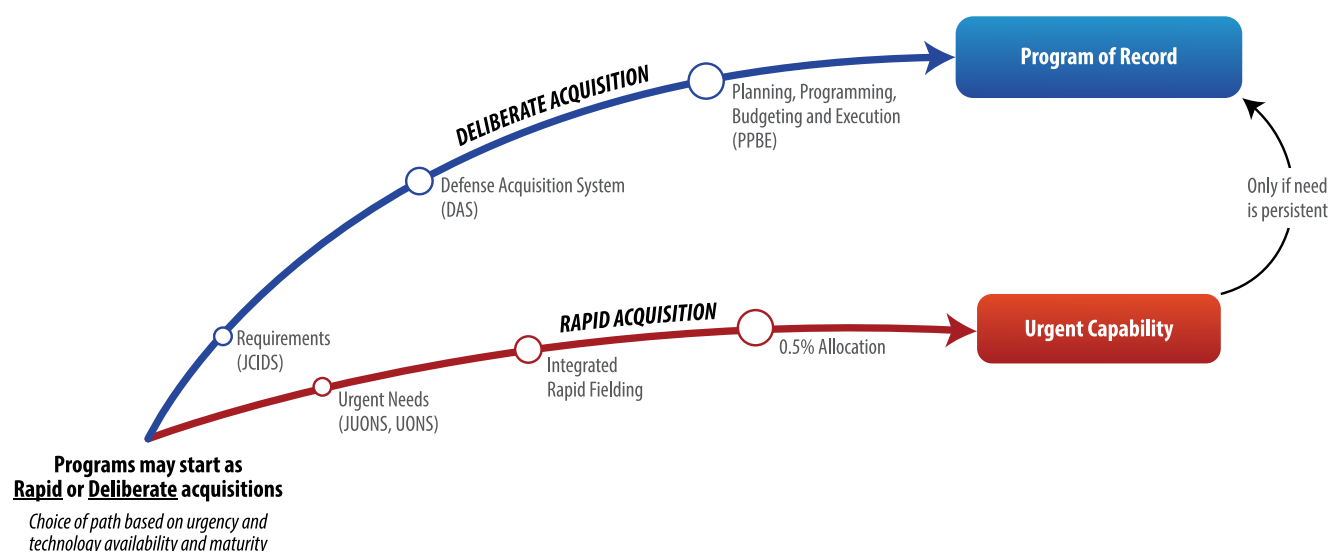
A dual acquisition process was proposed in the DSB Report on *Fulfillment of Urgent Operational Needs, 2009.*
Rapid acquisition process and programs are with us to stay and should be embraced by leadership.

multi-mission ("Swiss army knife-like") approach versus a simplified single mission approach ("plastic knife, fork, and spoon") and how much risk to assume versus the potential benefits to be accrued.

Rapid acquisition

A plethora of rapid acquisition organizations have proliferated around the Department outside the standard acquisition and requirements process. War fighter urgent operational needs drove these activities to go from a validated requirement to fielded capability in two years or less. Well-known operational problems that held such urgent operational needs and programs included the efforts to counter improvised explosive devices in Iraq and Afghanistan as well as delivering quickly battlefield surveillance capabilities.

Fast acquisition approaches maintain their own set of challenges, for example, once a rapid capability is fielded, the associated training, maintenance, and sustainment become the next set of challenges. The DoD also continually faces the challenge in determining the proper end state of a successful rapid acquisition program. How does the Department reconcile programs of record with their rapid acquisition adjuncts with what happens to the equipment when the urgent need is no longer there? One such example is the MQ-9 Reaper unmanned aircraft program and myriad of modifications to it driven by the Joint Urgent Operational Need process.

The closest to an underlying design metric for adaptive systems is speed; whenever feasible, capabilities should be fielded fast. Even if an attempted "80 percent solution" provided quickly to the war fighter fails, often the most adaptable approach is to rapidly try a different approach. For this reason, rapid acquisition processes and programs will stay with the DoD and Department leadership should embrace them.

Open and modular systems

DoD also needs to commit to open and modular building systems for those cases with impossible rapid fielding, such as the next generations of

ship, ground vehicle, or aircraft. The Department can achieve open standards a variety of ways, but there are fundamentals that cannot compromise. For example, the system module interfaces must be based on an agreed-upon standard available publicly; conversely, the interfaces and data models cannot be proprietary to only some vendors.

Acquisition strategies for open and modular systems should include regular block upgrades within the program schedule, with the initial version consisting of only those technologies and subsystems that are sufficiently mature and earned a prioritization from the warfighter. For the subsequent blocks, the acquisition strategy should be flexible to allow for unplanned changes due to emerging threat or technology requirements to guide specific content of each block. Finally, the system design should build in appropriate margins in size and weight, as well as "hooks" for future unknown design upgrades, such as hardened points on aircraft wings or extra payload volume on ships and submarines.

While having open, modular designs are critical for enabling adaptive systems, there must also be a deliberate technology maturation process to take advantage of the open system design. The Military Services need to continuously fund technology pipelines to feed future upgrades. Research and technology development must be resourced with a deliberate objective of feeding potential future block upgrades of systems. Experimenting and prototyping programs in the Department also should be used to mature concepts and capabilities for block upgrades; such experimentation and prototyping remains critical for future innovation, as noted in *Technology and Innovation Enablers for Superiority in 2030 (2012 summer study)*.

For more strategic investments such as the future of long-range strike or air dominance, the Department should continue to emphasize a "family of systems" portfolio of capabilities approach organized around the broad mission area and across platforms and Military Services. The Department should then take a proactive approach to shaping and preparing for future conditions with the way it manages the portfolio

as a whole. This includes deliberate hedges in the acquisition planning to defer final commitment in design and budgeting until it becomes clear exactly what capability is needed to hit a desired fielding date. Analysis tools to support hedging are believed to make such hedges in planning scientific and feasible.

Real-time adaptability is needed throughout the DoD

Most of the above has focused on the ability to upgrade systems rapidly over time as new threats demand and new technology provides opportunities. Another kind of system adaptability driven by unexpected events happens on the battlefield in the midst of conflict. This kind of adaptability requires overnight responses. The DSB has provided some guidelines on system architectures to achieve it; hooks, data recorders, and connectivity back to rapid analysis centers to understand what happened and craft responses; and the need for such permanent "on call" centers, such as the Joint Air Tactical Operations office for airborne electronic attack. The natural extension of this adaptability design principle is for the Department to continue to pursue, where feasible, real time adaptive capabilities; an example could be mission data files on aircraft having the ability for real-time as the EW threat environment is actually encountered during the mission.

Technology surprise is inevitable in a globalized world

How to obtain an edge for ourselves, how to anticipate an adversary's usage

The world is an unpredictable place, and the galloping advance of technology is making it more so. It has been experience multiple times that no matter how well DoD plans and prepares, there will be surprises—and there is the ever present value of inflicting surprise on our adversaries.

The DSB has advised DoD on how the Department can be better poised to respond to surprise swiftly and with agility, adaptability, and resilience. The approaches include having a

technology infrastructure which can be swiftly and inexpensively pivoted to meet changing needs and threats; using more red/blue teaming; and using realistic free play in training and exercises. The DSB has also identified potential technological surprises and recommended hedging strategies in certain circumstances.

An agile and responsive acquisition system acts as an enabler for preparing for surprise, and in particular an agile requirements regime based on early up front rational analysis of "what to buy" in contrast to "how to buy it." This encourages the creativity of the scientists and engineers in U.S. industry and universities. An innovative DoD should introduce change into the field: new potent systems, creative strategies and tactics, powerful operational concepts, outstanding Military Service personnel performance, at such a dizzying rate that an adversary could maintain no hope of developing countermeasures fast enough; this is the essence of how to ensure future U.S. military superiority.

A strong technology base, including knowledge of emerging science and technology, dedicated scientists and engineers, and infrastructure and facilities, acts as a solid foundation in the preparation for surprise. It provides the DoD both strategic differentiators and strategic necessities.

Of course, the U.S., the national security community, and the Military Services can and have experienced surprise in many ways. The potential opportunity and consequence of potentially devastating surprise, explored in the *Strategic Surprise (2014)* report, has only increased in the present day. Of the several reasons for the increases, almost none of them are new.

Scientific breakthroughs, rapid and unexpected technology development, and novel uses of existing capabilities all exemplify the ways the DoD thinks about technology surprise. Accelerating global advances in technology cause an increasing likelihood that potential adversaries may first discover and employ the technology surprise. This explains the desire in U.S. national security to find novel ways to make an early detection of a breakthrough, to understand and mitigate its

potential use by adversaries against the homeland, and the Department to exploit it for U.S. national interests. The DSB identified two categories of surprise: "known surprises" and "surprising surprises" in the *Capability Surprise (2008)* report: each requiring a different course of action to best mitigate, and each requiring persistent and focused leadership attention.

The known surprise category consists of cases where the country received clear and unambiguous warning that a serious, indeed possibly catastrophic condition was emerging, and which a potential adversary held good reason to pursue. Potential surprises that fit this category today are in the domains of cyber, space, and nuclear weapons. In these known surprise cases, the Department needs persistent leadership attention to assess and mitigate the constantly changing risks, to continually prepare using appropriate operational exercises and red teaming, and needs its leadership to track progress via a set of measurable goals.

Cases of surprising surprises occur when the nation might have access to the possible information indicating the eventual surprise, but was buried among myriad of other possibilities, any of which held unclear evidence and consequences. To address this difficult challenge of preparing for surprising surprises, the DSB identified five necessary capabilities: scanning and sifting processes, red capability projection, net assessment, options analysis, and finally a decision package to aid senior leadership in establishing a path forward.

A wide variety of technologies, capabilities, concepts, and enablers may be candidates for emerging challenges and opportunities. The Department could to define this topic area as the framework that asks: what are potential serious outcomes that the U.S. and the DoD would regret ten years forward, say in 2027, and what can the Department do to prevent them? Where should the U.S. develop capabilities now to best prepare for to avoid regret in the future? A number of candidate emerging opportunities and challenges have been identified with a summary listed as follows:

- Concepts for combined weapons effects and operations;

- New and innovative uses of autonomous systems;

- Continuing exploitation of the undersea domain in new ways;

- Holistic, end-to-end approaches to missile and cruise missile defense (including so called "left of launch");

- Approaches to disrupt adversary weapon systems, including asymmetric and/ or cost imposing strategies;

- Ensuring forces can fight through a nuclear event;

- Enhancing space security and resiliency;

- Developing an effective space control capability;

- Ensuring the trustworthiness and integrity of critical systems;

- Innovative concepts for combined, cognitive and adaptive electronic warfare, communications, and sensor capabilities; and

- Concepts for robust and resilient communications and position and navigation capabilities.

Rekindling a culture of innovation is a necessary step

The U.S. defense industrial base often receives criticism for high cost, excessive time to market, and lack of innovation. All tend to be true to a degree, certainly as compared to the commercial work place, but largely a consequence of the way its customer, the DoD acquisition system, buys its products. Requests for proposals for developmental systems generally specify general system and performance characteristics but all too often also specify design attributes that needlessly constrain technical approaches, getting in the way of innovation. Note the DoD can demand mature system designs in development acquisitions without being over-prescriptive of the design approach.

Because of a long history of cost and schedule overruns or serious performance underruns in

development programs, acquisitions can ask for detailed risk assessments and risk reduction plans and specify required technical readiness levels (TRLs) at relatively early in the development cycle. In fact the Department, driven in some cases by statute, developed a mechanical dependence on specifying early TRL sufficiency and compliance well beyond the original purpose of TRLs. Experienced design and development engineers in both military and commercial applications generally do not evaluate and mitigate technical risk by using something as superficial as a single TRL number assessment—indeed it is not in their internal vocabulary—yet that is what the current acquisition system and statute demands. While this may be reasonable as a way of calibrating competing proposals, there is no formal method in the evaluation process for the potential benefits associated with an innovative offering to be traded off with the higher associated risk. While true that there can be innovation that does not create risk for time or money, most often, with technical innovation, that is not the case. In general, an innovative solution, by definition, is not something that has been done before and does not have the same level of maturity as a "proven" way of doing things. Because the downside evaluation marks for risk are clear and the upside for added performance value or the benefits of some other beneficial characteristic are not, contractors are motivated to take the safe road; low risk at the expense of innovation.

In addition to the issue of real or perceived risk in proposal evaluation, major contractors often become concerned that the higher risk associated with some new way of doing things will come back to haunt them in subsequent competitive procurements. A standard section of a DoD request for proposals is "past performance," in which both the bidder, as well as government program managers, provide examples of previous similar development programs in which the bidder performed. If, as a result of trying to do something new, a bidder ran into cost or schedule trouble in a previous program, this could negatively affect their score on a new effort. In the technology development world, it

is standard practice, particularly in the case of one poor contract performance, to document lessons learned from the experience and describe how that learning will apply to a new effort. The current system incentivizes downplaying innovative or non-standard approaches.

The defense industrial base's innovation is also impacted by the inherent difference between very large companies, which the DoD relies on to produce systems at scale, and small companies, which tend to be more flexible and innovative. Many valid reasons exist for the lack of agility in larger companies, including the need for highly coordinated efforts across a large, sometimes geographically distributed workforce, driving the need for standard processes, as well as the sometimes huge financial impact of falling short. While this conservatism contributes to performance safety and stability, no doubt remains that it tends to inhibit innovation.

Many companies recognize this problem and attempt to isolate small development or prototyping organizations from the rest of the company. The isolation is not simply physical but also entails less bureaucracy, fewer processes, and greater incentives for "out of the box" thinking. Similarly, teaming with small centers of innovation during early development in an attempt to circumvent the significant cultural disconnect between small and large companies can disincentivize both to effectively work with each other. Lastly, a disconnect can also occur when an innovative component prototype transitions into a system that must reliably operate in the tough environments of combat, be operated by non-technical troops, and be sustained for years.

Thus, while the defense industrial base certainly desires greater innovation, one of the keys to achieving it is for greater innovation in the way the government specifies, evaluates, and works with contractors. Specifying how the potential fruits of innovation will be traded off with possible negative risk, cost, and schedule impacts would help. Specifying performance, cost and schedule objectives without creating an impression, real or imaginary, about "favored" solutions would

Surprise remains inevitable, may come in various forms, and may arise because of new technologies, new system constructs, or new ways of using existing systems, operating in new domains with new tactics and operations.

also help. Because one of the required attributes in a time of uncertainty on the battlefield is flexibility, the DoD must find ways to specify quantitatively what flexibility means in terms of a particular system, how it will evaluate and test the systems, and so on. Quantifying flexibility for the particular situation involved, specifying it as a key performance parameter, and describing the process for evaluating it through testing in competitive demonstrations may incentivize contractors to innovate and provide real system flexibility.

Planning for surprise is no mystery

Surprise remains inevitable, may come in various forms, and may arise because of new technologies, new system constructs, or new ways of using existing systems, operating in new domains with new tactics and operations. It can be reduced by paying attention to emerging technologies, watching ways in which potential adversaries operate and train, reading their publications, and thinking about how they might avoid U.S. strengths and exploit its weaknesses.

Two other aspects of surprise remain equally important—

- The DoD should assume that it will happen and create a culture of flexibility and adaptability in how it specifies and builds its systems, in how it trains the troops to fight, in how it uses new technologies, and in how it encourages and harnesses innovation.

- The Department should not think about surprise solely as the province of the adversary. It is the DoD's to exploit and inflict, and an opportunity to create uncertainty on adversary operations, impose cost, and weaken the ability to respond to U.S. initiatives.

Keys to achieving these objectives include aggressive red teaming; balancing risk with opportunity; encouraging diversity of thought and approaches; building a culture of innovation; seeking out and embracing new technologies; and fashioning systems that can be block upgraded in synchronization with the operational cycles of the troops that will use them, and whose system operations and algorithms can be altered literally overnight to mitigate problems or exploit opportunities that present themselves on the battlefield.

Supporting DSB reports

Transformation: A Progress Assessment (2005 summer study)

21st Century Strategic Technology Vectors (2006 summer study)

Challenges to Military Operations in Support of U.S. Interests (2007 summer study)

Creating an Effective National Security Industrial Base for the 21st century (2008)

Capability Surprise (2008 summer study)

Buying Commercial – Gaining the Cost/ Schedule Benefits for DoD Systems (2009)

Fulfillment of Urgent Operational Needs (2009)

Enhancing Adaptability of our Military Forces (Parts A and B) (2010 summer study)

Improvements to Services Contracting (2011)

Basic Research (2012)

Technology and Innovation Enablers for Superiority in 2030 (2012 summer study)

Strategic Surprise (2014 Summer Study)

A CALL TO ACTION

The seven defense priorities the Defense Science Board offers for the new Administration differ greatly in kind.

Protecting the homeland and deterring the use of nuclear weapons are core responsibilities and competences of the Department of Defense, and of the highest priority. Changing circumstances, new adversaries, and evolving technology present challenges the Department must and can meet.

The mission to support stabilization, reconstruction, peace keeping and nation building greatly differs from conflict with the armed forces of adversary states, a mission arisen again over the last hundred years, made even more difficult by the ineluctable accompanying insurgency. Gray zone conflicts also represent a very different mission than conventional war with adversary states, and will increasingly be the norm as other countries seek ways to avoid direct conflict with the potent U.S. armed forces, and yet accomplish their aggressive policy objectives.

Information and information technology stands at the heart of modern warfare for the United States and its adversaries. Information dominance must be a DoD goal as it is also a goal of adversaries.

Cyber, intelligence systems, and autonomy present a threat to mitigate and an opportunity to grasp; intelligent systems and autonomy are similar.

Finally, relative to all of the above, and more, the Department must be prepared to effectively respond to inevitable surprise, as well as cause surprise to deter and confound adversaries. Doing so partly depends on technology, even more on the way the Department works, and most of all on the Department culture. At the end of the day the DoD's culture of innovation will likely offer competitive military advantage as any technology or system.

By summarizing the main findings and recommendations of the Defense Science Board over the last dozen years, the Board intends this report to assist the incoming Administration to make a fast start in addressing pressing national security issues and opportunities.

PHOTOGRAPHY CREDITS

Ch1. pg 14. U.S. Army Spcs. Charles Friedrich and Brandon Birge, both with the 1140th Engineer Battalion, Missouri Army National Guard, fill sandbags to help with flood relief efforts in Dutchtown, Mo., April 22, 2013. The U.S. Coast Guard, Army Corps of Engineers and National Guard units responded to major flooding along rivers in the Midwest. (DoD photo by Michelle Queiser, U.S. Army National Guard/Released)

Ch 2. pg 22. U.S. Air Force B-2 Spirit bomber aircraft from Whiteman Air Force Base, Missouri, like the one pictured above, deploy to Andersen Air Force Base, Guam, as a routine deployment providing global strike capability and extended deterrence against potential adversaries in the Indo-Asia-Pacific region. (U.S. Air Force photo by Airman 1st Class Joel Pfiester/Released)

Ch 3. pg 30. Chinese dredging vessels are purportedly seen in the waters in the disputed Spratly Islands in the South China Sea in this still image from video taken by a P-8A Poseidon surveillance aircraft provided by the United States Navy, May 21, 2015.

Ch. 4 pg 36. U.S. Navy Fire Controlman 1st Class Aaron Tadlock monitors a radar console in the combat information center aboard the guided missile destroyer USS Donald Cook (DDG 75) in the Atlantic Ocean Feb. 3, 2014. The Donald Cook was underway in the U.S. 6th Fleet area of responsibility conducting a home port change from Naval Station Norfolk, Va., to Naval Station Rota, Spain. (DoD photo by Mass Communication Specialist Seaman Edward Guttierez III/Released)

Ch 5. pg 46. Hexacopter drones flying in the evening, Copyright 2013, Oktay Ortakcioglu, Ratoath, Ireland

Ch 6. pg 54. Khowst Province, Afghanistan " Pfc. Tullio Perez (near), Pfc. Ryan Lethem (middle), Pfc. Jared Bishop (far), all assigned to 2nd Platoon, Troop B, 1st Squadron, 33rd Cavalry Regiment, 3rd Brigade Combat Team "Rakkasans," 101st Airborne Division (Air Assault), use secure electronic enrollment kits to record data of the local population in Shamal District, Afghanistan, Jan. 10, 2013. The mission was conducted alongside soldiers with the Afghan National Army's 203rd Corps, 1st Brigade, 6th Kandak, 2nd Koy, in attempt to find anyone possibly working with insurgents within the district. (U.S. Army photo by Spc. Brian Smith-Dutton, Task Force 3/101 Public Affairs) (Photo Credit: Spc. Brian J. Smith Dutton (FORSCOM))

Ch 7. pg 62. *Fireball erupting in the South Tower,* Copyright 2001 – Robert J. Fisch